

CCNA 学习与实验指南

(640-802)

崔北亮 著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书通过配套光盘中的 1300 多分钟的视频讲解和近百个实验阐述了 CCNA 的各个知识点,不仅有助于读者对理论知识的学习,而且能够解决很多实际问题,提高读者的实践动手能力。精辟的真题解析更可以作为备考 CCNA 的冲刺指南。全书紧贴 640-802 考试大纲,全面而系统地分析和介绍了 CCNA 考试中涵盖的各个知识点。对每个知识点在考试中的重要程度均有标注,每章最后还有近期 CCNA 真题的解析。全书共分 22 章,内容涉及三大方面,局域网部分:网络互联基础知识和网络参考模型,思科路由器和交换机介绍,静态和动态路由协议(包括 RIP、EIGRP、OSPF)原理及配置,VLAN 和 VLAN 间路由的实现,CDP、VTP 和 STP 协议的使用,无线网络互联和 IPv6 等;广域网部分:广域网接入技术,PPP 和帧中继的使用,DHCP 和 NAT 等;网络安全部分:网络安全介绍,访问控制列表的使用和安全远程办公的实现等。

本书特别适用于那些渴望取得 CCNA 认证的读者,取得认证的同时,真正具备 CCNA 的能力;同时也可以作为高校计算机网络技术的教材,弥补实验设备的不足,改善现有学历教育重理论轻实践的现状;更是那些想掌握网络技术,提高动手能力,并能应用于实践的网络爱好者,难得一见的实验指导用书。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

CCNA 学习与实验指南 / 崔北亮著. —北京:电子工业出版社, 2010.9
ISBN 978-7-121-11572-1

I. ①C… II. ①崔… III. ①计算机网络—工程技术人员—资格考核—自学参考资料 IV. ①TP393

中国版本图书馆 CIP 数据核字(2010)第 155939 号

责任编辑:李 冰

印 刷:北京东光印刷厂

装 订:三河市皇庄路通装订厂

出版发行:电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本:787×1092 1/16 印张:37.25 字数:931 千字

印 次:2010 年 9 月第 1 次印刷

印 数:4000 册 定价:75.00 元(含光盘 1 张)

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010) 88254888。

质量投诉请发邮件至 zltz@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线:(010) 88258888。

前言

Cisco 公司的职业资格证书在全球一向都有“通往高薪直通车”的美誉，足见其含金量，并为众多用人单位所重视。获得思科认证意味着加入受到业界认可和尊敬的网络专业人士行列。通过本书内容的学习与掌握，对于拥有思科证书，成功的几率自然也就高出很多。

本书紧紧围绕思科 CCNA 最新考试科目 640-802 的考试大纲编写，与传统的教科书和一般的培训教材有本质的区别，它呈现给读者的不仅仅是一本教材，更是提供了一个综合的网络实验环境，仅仅通过一台电脑，便可以亲自动手完成本书涉及的所有路由器和交换机的实验配置及测试。多数 CCNA 教材也涉及实验配置，可读者往往因为没有足够的网络设备而只能望洋兴叹，学习的效果大打折扣。

本书结合实验对理论进行阐述，形象生动；每章最后的试题讲解都摘自 CCNA 考试的真题，并用本章学到的知识进行解答，帮助读者顺利通过考试；很多章节的实验更是从实际需求出发，拉近了读者和实践的距离，让读者成为真正的 CCNA；针对本书设计的实验机架，还可用于实际的工作环境中，解决读者没有路由器的苦恼。

限于作者水平和时间有限，一些小的错误在所难免，不足之处敬请谅解。

视频光盘

配套光盘中提供了 1300 多分钟的作者中文授课视频、补充资料、实验配置和故障排除场景。

本书涉及的所有应用程序和程序可以从作者的个人主页 <http://blcui.njut.edu.cn/ccnanew.rar> 处下载。为了便于读者能更好地阅读此书，相互交流，作者个人主页上开通了讨论版，网址是 <http://blcui.njut.edu.cn/bbs>。

本书目的

本书不但教授思科的网络技术，而且有助于读者熟悉 CCNA 考试套路，帮助读者顺利通过 CCNA 考试。更为主要的是，本书还将培养读者的动手能力和实践水平，把读者培养成为一名真正的 CCNA，而不仅仅是一纸证书。

本书是作者历时 1 年精心编著而成的，呈现给读者的不仅是一本教材，更是提供了一个综合的网络实验环境，便于读者在此之上深入领会网络技术的精髓。仅仅通过一台电脑，便可以虚拟出多台路由器、交换机和集线器，并能将它们完美地结合在一起，完成书中涉及的几乎所有路由和交换的实验配置及测试。

本书内容

本书通过理论讲解，视频演示，真题解析和大量的动手实验，目的是培养出真正的 CCNA。全书紧贴 640-802 考试大纲，全面而系统地分析和介绍了 CCNA 考试中涵盖的各个知识点。对每个知识点在考试中的重要程度均有标注，每章最后还有近期 CCNA 真题的解析。全书共分 22 章，内容涉及三大方面，局域网部分：网络互联基础知识和网络参考模型，思科路由器和交换机介绍，静态和动态路由协议（包括 RIP、EIGRP、OSPF）原理及配置，VLAN 和 VLAN 间路由的实现，CDP、VTP 和 STP 协议的使用，无线网络互联和 IPv6 等；广域网部分：广域网接入技术，PPP 和帧中继的使用，DHCP 和 NAT 等；网络安全部分：网络安全介绍，访问控制列表的使用和安全远程办公的实现等。

读者对象

本书特别适用于那些渴望取得 CCNA 认证的读者，取得认证的同时，真正具备 CCNA 的能力；同时也可以作为高校计算机网络技术的教材，弥补实验设备的不足，改善现有学历教育重理论轻实践的现状；更是那些想掌握网络技术，提高动手能力，并能应用于实践的网络爱好者，难得一见的实验指导用书。

CCNA 考试重点的表述

书中对每个章节和分段的重要程度均用星号来表示，***表示很重要，**表示重要，*表示不太重要，没有*表示该章节或段落在 CCNA 考试中几乎不会出现。CCNA 考试中不会出现的内容并不表示在实践中用不到，相反，书中所列的不涉及 CCNA 考试的内容多是实践中经常要用到的知识或技能。

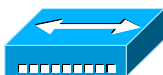
本书命令句法表示习惯

- 本书对多数配置命令均加底纹表示；
- 对配置命令的解释以底纹加斜体表示；
- 对查看命令及其输出以 Courier New 字体表示，着重要突出的部分以黑体显示；
- 竖线“|”用于分隔可选的、互斥的选项；
- 方括号“[]”表示任选项；
- 花括号“{ }”表示必选项。

思科图标示例

思科公司使用一套标准化的图标来表示在网络拓扑图中的各种设备。在本书和 CCNA

考试中使用的图标如下：



10Mbps 集线器



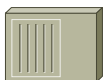
100Mbps 集线器



网桥



二层交换机



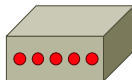
集线器



无线 AP



路由器



调制解调器



PC



服务器



笔记本电脑



多层交换机



路由交换机



防火墙



无线路由器



网云



无线



串行线



以太网



虚电路

目 录

第 1 章	CCNA 认证知识	1	2.4.2	网际层***	28
1.1	Cisco 认证体系	1	2.4.3	传输层***	32
1.2	CCNA 认证介绍	3	2.4.4	应用层***	36
1.2.1	考试代号	3	2.5	IP 地址***	36
1.2.2	考试大纲	3	2.5.1	二进制和十进制间的转换***	36
1.3	CCNA 考试相关内容	6	2.5.2	IP 地址分类***	37
1.3.1	考点查询	6	2.5.3	保留 IP 地址***	38
1.3.2	考试登记	6	2.5.4	公有 IP 地址和私有 IP 地址**	38
1.3.3	考前问卷调查	6	2.5.5	IP 子网划分***	39
1.3.4	正式考试	7	2.6	封装和解封装***	44
1.4	CCNA 证书相关内容	7	2.7	真题精选***	48
1.4.1	考后注册	8	2.8	真题解答***	59
1.4.2	证书的重发	8	第 3 章	以太网*	69
1.4.3	证书的有效期限	8	3.1	以太网简介*	69
第 2 章	网络互联和参考模型***	9	3.2	以太网帧*	72
2.1	网络的分类**	9	3.3	真题精选*	75
2.1.1	按覆盖范围分*	9	3.4	真题解答*	75
2.1.2	按拓扑结构分*	10	第 4 章	思科路由器**	77
2.1.3	按传输介质分***	11	4.1	模拟设备的使用	77
2.1.4	按服务方式分*	14	4.1.1	Packet Tracer 模拟器的使用	77
2.2	网络体系结构	15	4.1.2	用“Dynamips”搭建 CCNA 实验台	83
2.3	ISO/OSI 参考模型***	17	4.2	路由器简介**	87
2.3.1	物理层***	18	4.2.1	路由器的基本硬件组成**	87
2.3.2	数据链路层***	19	4.2.2	路由器的引导过程***	89
2.3.3	网络层***	23	4.2.3	show version 命令***	92
2.3.4	传输层***	24	4.2.4	路由器外观*	93
2.3.5	会话层***	25	4.3	路由器的一般操作***	94
2.3.6	表示层***	25	4.3.1	控制台连接***	95
2.3.7	应用层***	25	4.3.2	Setup 模式*	96
2.4	TCP/IP 参考模型***	26			
2.4.1	网络访问层***	28			

4.3.3	路由器的操作模式**	98
4.3.4	命令行接口**	99
4.3.5	路由器常用配置***	102
4.4	简单网络的配置、管理和排错**	108
4.4.1	配置和排错**	108
4.4.2	文件管理***	115
4.5	CDP 协议**	118
4.5.1	CDP 介绍**	118
4.5.2	CDP 应用**	119
4.6	真题精选***	122
4.7	真题解答***	129

第 5 章 路由选择协议*** 133

5.1	路由基础**	133
5.1.1	网络互连*	133
5.1.2	路由原理*	134
5.1.3	路由协议***	136
5.2	直连路由**	137
5.3	静态路由***	140
5.3.1	配置静态路由***	140
5.3.2	静态路由的优缺点**	143
5.4	默认路由**	144
5.5	动态路由协议***	146
5.5.1	静态路由与动态路由的比较**	146
5.5.2	管理距离***	147
5.5.3	路由选路原则***	147
5.5.4	距离矢量和链路状态路由协议***	148
5.5.5	常见的路由协议**	151
5.6	真题精选***	153
5.7	真题解答***	157

第 6 章 RIP*** 160

6.1	RIP 概述***	160
6.1.1	RIP 主要特征***	160
6.1.2	RIP 拓扑变化**	161
6.1.3	RIP 定时器***	162
6.2	RIP 配置**	163

6.3	VLSM 和 CIDR***	173
6.3.1	VLSM***	174
6.3.2	CIDR***	177
6.4	RIPv2***	177
6.4.1	RIPv1 的局限性***	178
6.4.2	RIPv2 的增强特性**	183
6.4.3	RIPv2 的配置**	183
6.4.4	常见路由协议的比较**	191
6.5	路由查找***	192
6.5.1	路由表结构**	192
6.5.2	路由查找过程***	194
6.6	真题精选***	195
6.7	真题解答***	200

第 7 章 EIGRP*** 204

7.1	EIGRP 概述和基本配置***	204
7.1.1	EIGRP 特性***	204
7.1.2	EIGRP 包格式*	205
7.1.3	EIGRP 分组类型**	206
7.1.4	EIGRP 表***	209
7.1.5	EIGRP 度量值计算**	213
7.2	DUAL 算法和 EIGRP 排错**	216
7.2.1	DUAL 相关术语和 EIGRP 排错***	216
7.2.2	DUAL 算法**	222
7.3	EIGRP 高级配置**	224
7.3.1	EIGRP 非等值负载均衡	224
7.3.2	EIGRP 汇总***	226
7.3.3	EIGRP 外部路由*	229
7.3.4	EIGRP 验证*	230
7.3.5	EIGRP 性能调整*	231
7.4	真题精选***	231
7.5	真题解答***	234

第 8 章 OSPF*** 237

8.1	链路状态路由协议**	237
8.1.1	链路状态路由协议介绍**	237
8.1.2	链路状态路由协议工作过程**	237
8.1.3	链路状态路由协议的优缺点**	238

8.2	OSPF 概述和基本配置***	239	第 10 章	VLAN***	298
8.2.1	OSPF 特性***	239	10.1	VLAN 介绍**	298
8.2.2	OSPF 术语**	239	10.1.1	VLAN 的由来*	298
8.2.3	OSPF 包格式*	241	10.1.2	VLAN 的优点**	299
8.2.4	OSPF 包类型***	241	10.2	VLAN 干线***	300
8.2.5	OSPF 邻居关系的建立**	243	10.2.1	什么是干线**	300
8.2.6	OSPF 基本配置***	245	10.2.2	干线协议**	301
8.2.7	DR 和 BDR***	247	10.2.3	交换机间 VLAN 的通信过程***	302
8.2.8	OSPF 度量值计算*	252	10.2.4	DTP 协议***	304
8.3	OSPF 高级配置**	253	10.3	配置 VLAN***	305
8.3.1	OSPF 验证*	253	10.3.1	配置单台交换机上的 VLAN***	306
8.3.2	OSPF 默认路由***	255	10.3.2	配置 Trunk***	310
8.3.3	RIP 升级到 OSPF**	256	10.3.3	本地 VLAN**	312
8.3.4	OSPF 故障排除**	260	10.3.4	语音 VLAN*	313
8.4	真题精选***	268	10.3.5	维护 VLAN 信息**	314
8.5	真题解答***	272	10.3.6	用 Dynamips 模拟器配置 VLAN*	317
第 9 章	交换机**	276	10.4	VLAN 间路由***	320
9.1	局域网设计**	276	10.4.1	基于路由器物理接口的 VLAN 间路由**	320
9.1.1	分级网络设计**	276	10.4.2	基于路由器子接口的 VLAN 间路由***	321
9.1.2	交换机选型*	278	10.4.3	交换机上的端口类型*	322
9.2	交换机分类*	279	10.4.4	基于三层交换机的 VLAN 间路由	324
9.2.1	根据转发方式分***	279	10.4.5	路由器和三层交换机在实现 VLAN 间路由上的差异	326
9.2.2	根据对称性分*	280	10.5	VLAN 故障排除**	327
9.2.3	根据缓存方式分*	281	10.6	真题精选***	332
9.2.4	根据功能层分*	281	10.7	真题解答***	337
9.3	交换机基本配置**	281	第 11 章	VTP**	341
9.3.1	与路由器的相似之处*	281	11.1	VTP 介绍***	341
9.3.2	交换机的图形化管理工具	282	11.1.1	VTP 的作用***	341
9.3.3	交换机的远程登录**	282	11.1.2	VTP 的特点***	341
9.3.4	交换机的维护和查看命令**	285	11.1.3	默认 VTP 信息**	341
9.4	交换机的安全配置**	286	11.1.4	VTP 域名 (Domains) **	342
9.4.1	交换机密码安全*	286			
9.4.2	交换机易受到的安全威胁*	286			
9.4.3	交换机的安全防御*	289			
9.5	真题精选***	293			
9.6	真题解答***	295			

11.1.5	VTP 通告 (Advertising) *	345	13.3.1	配置 Linksys**	394
11.1.6	VTP 模式 (Modes) ***	346	13.3.2	配置无线网卡*	399
11.1.7	VTP 裁剪 (Pruning) **	346	13.3.3	Packet Tracer 中配置 Linksys*	400
11.2	VTP 配置与排错**	349	13.4	无线故障排除**	401
11.2.1	VTP 配置的注意事项**	349	13.5	真题精选***	403
11.2.2	VTP 配置**	350	13.6	真题解答***	405
11.2.3	VTP 排错**	351			
11.3	真题精选***	353	第 14 章	广域网**	407
11.4	真题解答***	356	14.1	广域网概述**	407
第 12 章	STP***	358	14.1.1	广域网设备*	407
12.1	冗余拓扑中存在的问题***	358	14.1.2	广域网拓扑***	407
12.2	STP 介绍***	361	14.1.3	广域网链路的类型**	409
12.2.1	STP 算法***	362	14.1.4	广域网帧的封装格式***	410
12.2.2	BPDU**	366	14.2	广域网技术**	411
12.2.3	端口角色***	367	14.2.1	广域网技术分类**	411
12.2.4	端口状态和 BPDU 时间***	367	14.2.2	广域网接入技术介绍*	412
12.3	STP 收敛***	369	14.3	真题精选***	415
12.3.1	生成树的选举***	369	14.4	真题解答***	418
12.3.2	STP 拓扑变化**	372	第 15 章	PPP**	420
12.3.3	增强的 STP 功能**	373	15.1	PPP 概述**	420
12.4	高级的 STP***	374	15.1.1	HDLC**	420
12.4.1	PVST+**	374	15.1.2	同步和异步串行通信*	421
12.4.2	RSTP**	376	15.1.3	PPP 特点**	421
12.5	真题精选***	378	15.1.4	PPP 分层体系结构***	422
12.6	真题解答***	380	15.1.5	PPP 会话建立过程*	423
第 13 章	无线网络***	383	15.1.6	PPP 身份验证协议***	424
13.1	无线网络介绍**	383	15.2	配置 PPP**	426
13.1.1	使用无线网络*	383	15.2.1	PPP 基本配置**	426
13.1.2	无线局域网标准***	385	15.2.2	PPP 验证配置***	428
13.1.3	无线局域网的组件*	387	15.3	真题精选***	431
13.1.4	实施无线***	388	15.4	真题解答***	431
13.1.5	规划无线局域网*	391	第 16 章	帧中继***	432
13.2	无线局域网安全***	391	16.1	帧中继概述***	432
13.2.1	无线网的安全威胁*	392	16.1.1	帧中继优点*	432
13.2.2	无线网安全协议**	392	16.1.2	帧中继术语***	433
13.2.3	加强无线网安全*	394	16.1.3	帧中继运行方式*	437
13.3	配置无线局域网*	394	16.1.4	帧中继寻址***	439
			16.1.5	水平分割问题***	441

16.2	配置帧中继***	441	18.1.4	一般防范攻击的技术*	489
16.2.1	帧中继基本配置**	442	18.1.5	网络安全车轮 (Network Security Wheel) *	490
16.2.2	RIP over 帧中继**	445	18.2	路由器的安全**	491
16.2.3	帧中继子接口**	448	18.2.1	密码安全*	491
16.3	真题精选***	451	18.2.2	限制远程访问**	491
16.4	真题解答***	455	18.2.3	记录日志**	494
第 17 章	访问控制列表***	458	18.2.4	禁用不需要的服务或端口*	495
17.1	ACL 概述**	458	18.3	SDM *	496
17.1.1	ACL 定义**	458	18.3.1	SDM 的关键特性	496
17.1.2	ACL 作用**	458	18.3.2	配置 SDM	498
17.1.3	ACL 工作流程***	459	18.4	路由器的文件管理 *	501
17.1.4	ACL 类型**	460	18.4.1	IOS 文件管理	501
17.2	标准 ACL**	460	18.4.2	配置文件管理*	504
17.2.1	通配符掩码***	460	18.5	密码恢复技术 ***	505
17.2.2	配置标准 ACL**	461	18.5.1	路由器密码恢复***	505
17.2.3	编辑标准 ACL**	463	18.5.2	交换机密码恢复*	507
17.2.4	标准 ACL 放置的位置***	463	18.6	真题精选***	508
17.2.5	配置标准命名 ACL**	464	18.7	真题解答***	510
17.3	扩展 ACL***	465	第 19 章	远程办公*	512
17.3.1	配置扩展 ACL***	465	19.1	远程办公的商业需要	512
17.3.2	扩展 ACL 放置的位置***	467	19.1.1	远程办公的优势	512
17.3.3	扩展 ACL 的增强编辑功能*	467	19.1.2	远程办公的解决方案	512
17.3.4	扩展 ACL 中的 established**	468	19.2	宽带服务*	513
17.3.5	配置扩展命名 ACL**	470	19.3	VPN **	515
17.4	配置 ACL 的注意事项***	470	19.3.1	VPN 优点**	515
17.5	复杂 ACL	472	19.3.2	VPN 类型**	515
17.5.1	反射 ACL	473	19.3.3	VPN 安全性***	516
17.5.2	动态 ACL	475	19.3.4	IPSec 安全协议**	519
17.5.3	基于时间的 ACL	478	19.3.5	VPN 配置*	519
17.6	真题精选***	479	19.4	真题精选*	525
17.7	真题解答***	483	19.5	真题解答*	527
第 18 章	网络安全**	486	第 20 章	DHCP 和 NAT***	529
18.1	网络安全介绍*	486	20.1	DHCP**	529
18.1.1	网络安全的重要性*	486	20.1.1	使用 DHCP 的好处**	529
18.1.2	一般的安全威胁*	487	20.1.2	BOOTP 和 DHCP 的区别与联系**	529
18.1.3	网络攻击类型**	488			

20.1.3	DHCP 工作过程**	530
20.1.4	配置 DHCP 服务器和 客户端***	533
20.1.5	配置 DHCP 中继服务*	535
20.1.6	使用 SDM 配置 DHCP	536
20.2	NAT***	536
20.2.1	私有地址和公共地址***	536
20.2.2	什么是 NAT***	538
20.2.3	使用 NAT 的优点和 缺点***	538
20.2.4	配置静态 NAT**	539
20.2.5	配置动态 NAT**	541
20.2.6	配置 NAT 超载***	543
20.2.7	配置端口映射**	544
20.3	真题精选***	544
20.4	真题解答***	548

第 21 章	IPv6***	551
21.1	IPv6 的重要性***	551
21.2	IPv6 地址***	552
21.2.1	IPv6 地址表示***	552
21.2.2	IPv6 地址类型***	553
21.2.3	配置 IPv6 地址*	554
21.3	IPv6 路由*	555
21.4	IPv6 过渡策略***	558
21.5	真题精选*	560
21.6	真题解答*	562
第 22 章	综合实验***	564
22.1	实验要求**	564
22.2	实验配置***	566
22.3	真题精选***	576
22.4	真题解答***	579

第 1 章

CCNA 认证知识

随着人类步入信息社会，全球性的计算机网络——Internet 正在走进人们的工作、学习和生活，成为如同水、电和天然气一样的社会公共基础设施。自然，社会也对网络行业岗位提出了技术和技能要求。对于那些筹划建网的单位而言，当然希望由专业精通、经验丰富的高级工程师进行网络规划设计，使设计方案能够满足日益增长的用户需求并适应网络技术的发展；对于那些正在建设或已经建成网络的单位而言，当然希望聘用掌握知识、熟悉产品的技术人员安装、调试、运行和维护投入大笔资金建成的网络，使其发挥最大效益。为此，网络领域著名的厂商——Cisco（思科）公司推出了针对其产品的网络规划和网络支持工程师资格认证。

Cisco 公司的职业资格证书在国内外一向都有“通往高薪直通车”的美誉，虽然在国内由于种种原因，已经不像前几年一样火爆（一个最主要的原因是因为多数人都是通过背题而取得认证，并不具备真正的能力，本书不仅可以帮助读者通过 CCNA 认证，而且可以让读者成为真正的 CCNA），但其含金量还是为众多用人单位所重视，获得任何级别的思科认证均意味着加入受到业界认可和尊敬的熟练网络专业人士的行列。拥有思科证书，成功的几率自然也就高出很多。然而更多的人对于 Cisco 认证根本不了解，或者只了解其中的一点点，本章介绍 Cisco 认证考试的相关知识。



1.1 Cisco 认证体系

Cisco 认证是互联网界具有极大声望的网络技能认证。其总体认证体系包括路由和交换网络支持（售后工程师认证体系）、路由和交换网络设计（售前工程师认证体系）。同时，Cisco 公司还有网络安全、存储、语音和电信运营商方面的认证。

（1）认证证书分为三个等级

- 等级 1——工程师（Associate）
- 等级 2——资深工程师（Professional）
- 等级 3——网络专家（Expert）

（2）工程师认证有两种

- CCNA（Cisco Certified Network Associate，思科认证网络工程师）。
- CCDA（Cisco Certified Design Associate，思科认证设计工程师），表示在设计思科网络基础设施方面具备基本的或者初步的知识。拥有 CCDA 认证的人士可以为企业和机构设计包含 LAN、WAN 和拨号接入服务的路由和交换网络基础设施。

（3）资深工程师认证有五种

- CCNP（Cisco Certified Network Professional，思科认证资深网络工程师），该级别的

网络工程师具有对从 100 个到 500 个结点的融合式局域网和广域网进行安装、配置和排障的能力。获得 CCNP 认证资格的网络人士拥有丰富的知识和技能，能够管理构成网络核心的路由器和交换机，以及将语音、无线和安全集成到网络之中的边缘应用。

- **CCDP**（Cisco Certified Design Professional，思科认证资深设计工程师），表示精通或者熟知网络设计知识。获得 CCDP 认证资格的网络人士能够设计包含局域网、广域网和拨号接入服务的路由和交换网络，采用模块化设计方法，以及确保整个解决方案出色地满足业务和技术需求，且具有高可用性。
- **CCSP**（Cisco Certified Security Professional，思科认证资深安全工程师），表示精通或者熟知思科网络的安全知识。获得 CCSP 认证资格的网络人士能够保护和管理网络基础设施，以提高生产率和降低成本。认证内容侧重于安全 VPN 管理、思科自适应安全设备管理器（ASDM）、PIX 防火墙、自适应安全设备（ASA）、入侵防御系统（IPS）、思科安全代理（CSA）和怎样将这些技术集成到一个统一的集成化网络安全解决方案之中等主题。
- **CCIP**（Cisco Certified Internetwork Professional，思科认证资深互联网工程师），旨在证明就职于电信运营机构网络人士在基础设施 IP 网络解决方案方面具备的能力。具有 CCIP 资格的人士非常了解电信运营商领域涉及的网络技术，包括 IP 路由、IP QoS、BGP 和 MPLS。
- **CCVP**（Cisco Certified Voice Professional，思科认证资深语音工程师），目前负责将语音技术集成到底层网络架构中的 IT 人士正日益变得重要。获得 CCVP 认证资格的人士能够帮助创建一个透明、易于扩展和管理的语音解决方案。CCVP 认证表示非常精通融合式 IP 网络的实施、运行、配置和排障。认证内容侧重于 Cisco Systems CallManager、服务质量（QoS）网关、关守、IP 电话、语音应用、思科路由器及 Cisco Catalyst 交换机上的应用等主题。

(4) 网络专家认证有五种

- **CCIE**（Cisco Certified Internetwork Expert，Cisco 认证互联网专家）——路由和交换。路由和交换领域的 CCIE 认证资格表示网络人士在不同的 LAN、WAN 接口和各种路由器、交换机的联网方面拥有专家级知识。
- **CCIE**——安全。安全领域的 CCIE 认证表示网络人士在 IP 和 IP 路由，以及特定的安全协议和组件方面拥有专家级知识。
- **CCIE**——电信运营商。电信运营商 CCIE 认证（以前被称为通信和服务）表示网络人士在 IP 原理和核心 IP 技术（例如单播 IP 路由、QoS、组播、MPLS、MPLS VPN、流量工程和多协议 BGP）方面拥有专家级知识，并且在至少一项与电信运营商有关的网络领域具有专业知识。
- **CCIE**——存储网络。存储网络领域的 CCIE 认证表示网络人士在利用多种传输方式（例如光纤通道、iSCSI、FCIP 和 FICON）扩展网络基础设施上采用智能存储解决方案方面拥有专家级知识。
- **CCIE**——语音。语音领域的 CCIE 认证表示网络人



图 1-1-1 售后工程师认证金字塔

士在用于企业的 VoIP 解决方案方面拥有专家级知识。考生应当能够在 IP 网络上安装、配置和维护语音解决方案。

(5) 网络支持证书部分 (Cisco 售后工程师认证体系)

在前面这些认证考试中, 目前国内外需求量最大、参加人数最多的是路由和交换网络支持认证, 即 Cisco 售后工程师认证体系。目前其在国内的市场也日渐扩大, 总体架构呈金字塔形, 如图 1-1 所示, 从塔底到塔尖分别为: CCNA、CCNP、CCIE。



1.2 CCNA 认证介绍

CCNA 是思科认证网络工程师综合考试, 学习 CCNA 是增长网络知识, 检验网络技术, 提高自身价值, 通向专业认证道路的第一步。该认证考试要求考生必须拥有对中小型企业分支网络的安装、操作和排错能力。考试内容包括: 广域网 (WAN) 的连接、网络安全实施、网络类型、网络介质、路由和交换原理、TCP/IP 和 OSI 参考模型、IP 地址、WAN 技术、操作和配置路由和交换设备、通过虚拟局域网 (VLAN) 来扩展交换网络、配置 IP 路由、用访问控制列表来管理 IP 流量、建立点到点的连接以及建立帧中继连接等。

1.2.1 考试代号

CCNA 认证从设立至今, 其考试项目经历了多次的升级, 从最早 1998 年起设立的 640-407 改为 640-507 (2000 年 8 月起生效), 2002 年 4 月改为 640-607, 2003 年 9 月又更改为 640-801。Cisco 在 2007 年 8 月 1 日公布最新的 CCNA 考试为 642-802, 增加了部分关于 WLAN 和 WiFi 的内容, 这是近 4 年来 CCNA 考试的最大变动。同时 640-801 考试也是持续时间最长的 CCNA 考试。

1.2.2 考试大纲

CCNA640-802 是思科认证网络工程师综合考试。以下描述 CCNA 考试的一般标准内容, 其他相近的内容也会在考试当中出现, 为了更好地反映考试的内容和明确考试的目的, 下面的内容会随时更改而不另行通知。

1. 描述网络工作的原理

- 清楚主要网络设备的用途和功能;
- 可以根据网络规格需求选择组件;
- 用 OSI 和 TCP/IP 模型及相关的协议来解释数据是如何在网络中传输的;
- 描述常见的网络应用程序, 包括网页应用程序;
- 描述 OSI 和 TCP/IP 模型下协议的用途和基本操作;
- 描述基于网络的应用程序 (IP 音频和 IP 视频) 的效果;
- 解释网络拓扑图;
- 决定跨越网络的两个主机间的网络路径;
- 描述网络和互联通信的结构;
- 用分层模型的方法识别和改正位于 1、2、3 和 7 层的常见网络故障;
- 区分广域网和局域网的作用和特征。

2. 配置、检验和检修 VLAN 和处于交换通信环境的交换机

- 选择适当的介质、线缆、端口和连接头来连接交换机跟主机或者其他网络设备；
- 解释以太网技术和介质访问控制方法；
- 解释网络分段和基础流量管理的概念；
- 解释基础交换的概念和思科交换机的作用；
- 完成并检验最初的交换配置任务，包括远程访问控制；
- 用基本的程序（包括：ping、tracert、telnet、SSH、arp、ipconfig）和 show，以及 debug 命令检验网络和交换机的工作状态；
- 识别、指定和解决常见交换网络的介质问题、配置问题、自动协商和交换硬件故障；
- 描述高级的交换技术（包括：VTP、RSTP、VLAN、PVSTP、802.1q）；
- 描述 VLAN 如何创建逻辑隔离网络和它们之间需要路由的必要性；
- 配置、检验和检修 VLAN；
- 配置、检验和检修思科交换机的 trunking；
- 配置、检验和检修 VLAN 间路由；
- 配置、检验和检修 VTP；
- 配置、检验和检修 RSTP 功能；
- 通过解释各种情况下 show 和 debug 命令的输出，来确定思科交换网络的工作状态；
- 实施基本的交换机安全策略（包括：端口安全、聚合访问、除 VLAN1 之外的其他 VLAN 的管理等）。

3. 在中等规模的公司分支办公室网络中实现满足网络需求的 IP 地址规划及 IP 服务

- 描述使用私有 IP 和公有 IP 的作用和好处；
- 解释 DHCP 和 DNS 的作用和优点；
- 在路由器上配置、检验和排错 DHCP 和 DNS 操作（包括：命令行方式和 SDM 方式）；
- 为局域网环境的主机实施静态和动态 IP 地址服务；
- 在支持 VLSM（变长子网掩码）的网络中计算并应用 IP 地址规划；
- 使用 VLSM 和地址汇总决定合适的无类地址规划，以满足不同局域网/广域网的地址规划要求；
- 描述在与 IPv4 网络共存情况下实施 IPv6 的技术要求（包括：协议方式、双栈方式、隧道方式）；
- 描述 IPv6 地址；
- 鉴定并纠正普通的 IP 地址和主机配置问题。

4. 基本的路由器操作和路由的配置、检查和排错

- 描述路由的基本概念（包括：IP 数据包转发、路由查询）；
- 描述思科路由器的运作过程（包括：路由器初始启动过程、POST 加电自检、路由器的物理组成）；
- 选择适当的介质、线缆、端口和连接器将路由器连接到其他的网络设备和主机；
- RIPv2 的配置、检查和排错；
- 访问路由器并配置基本的参数（包括：命令行方式和 SDM 方式）；
- 连接、配置并检查设备接口的工作状态；

- 检查设备的配置并使用 ping、traceroute、telnet、SSH 等命令检验网络连接性；
- 在给定的路由需求下实施并检验静态路由和默认路由的配置；
- 管理 IOS 配置文件（包括：保存、修改、更新和恢复）；
- 管理思科 IOS；
- 比较不同的路由实现方法和路由协议；
- OSPF 配置、检查和排错；
- EIGRP 配置、检查和排错；
- 检查网络连接性（包括：使用 ping、traceroute、telnet、SSH 等命令）；
- 路由故障排错；
- 使用 show 和 debug 命令检查路由器的硬件及软件运作状态；
- 实施路由器安全。

5. 解释并选择适当的可管理无线局域网（WLAN）任务

- 描述跟无线有关的标准（包括：IEEE、WiFi 联盟、ITU/FCC）；
- 识别和描述小型无线网络组成结构的用途（包括：SSID、BSS、ESS）；
- 确定无线网络设备的基本配置以保证它连接到正确的接入点；
- 比较不同无线安全协议的特性及性能（包括：开放、WPA、WEP-1/2）；
- 认识在无线局域网实施过程中的常见问题（包括：接口、配置错误）。

6. 识别网络安全威胁和描述减轻这些威胁的一般方法

- 描述当前的网络安全威胁并解释实施全面的安全策略以降低安全威胁的必要性；
- 解释降低网络设备、主机和应用所遭受安全威胁的一般方法；
- 描述安全设备和应用软件的功能；
- 描述安全操作规程建议（包括网络设备的初始安全配置）。

7. 在中小型企业分支办公网络中实施、检验和检修 NAT 和 ACL

- 描述 ACL 的作用和类型；
- 配置和应用基于网络过滤要求的 ALC（包括：命令行方式和 SDM 方式）；
- 配置和应用 ALC 以限制对路由器的 telnet 和 SSH 访问（包括：命令行方式和 SDM 方式）；
- 检查和监控网络环境中的 ACL；
- ACL 排错；
- 描述 NAT 基本运作原理；
- 配置基于给定网络需求的 NAT（包括：命令行方式和 SDM 方式）；
- NAT 排错。

8. 实施和校验 WAN 连接

- 描述连接到广域网的不同方式；
- 配置并检查基本的广域网串行连接；
- 在思科路由器上配置并检查帧中继；
- 广域网实施故障排错；
- 描述 VPN（虚拟专用网）技术（包括：重要性、优点、影响、组成）；

- 在思科路由器间配置并检查 PPP 连接。



1.3 CCNA 考试相关内容

掌握 CCNA 考试的知识点后, 接下来就是参加 CCNA 考试, 首先查询考点, 进行考试登记, 回答考前问卷调查, 进入正式考试。

1.3.1 考点查询

从 2007 年 8 月 1 日起, Pearson VUE 在全球独家发送思科认证考试。在中国大陆, 位于 14 个城市的 17 家考试中心成为首批思科认证考试的授权考试中心, 为考生提供优质的考试服务。所有的思科考试中心均安装了生物检测设备, 如指纹采集、数码照相、电子签名设施等, 并按照新的要求实行严密的摄像监控。

考生可以采用以下方式注册考试:

(1) 联系考试中心, 咨询有关考试注册、付款、预约等事宜。

(2) 登录 <http://www.pearsonvue.com/>, 在网上注册考试。网上注册需要使用信用卡以美元价格支付考试费。

(3) 致电 Pearson VUE 客服中心 400 880 5123, 注册考试。通过呼叫中心注册需要使用信用卡以美元价格支付考试费。

Pearson VUE 将在遵照思科公司要求的前提下, 尽量扩大思科考试中心的覆盖范围, 更好地为广大考生提供考试服务。请考生密切关注 VUE 网站, 了解思科考试中心的最新信息, 在自己最方便的考试中心参加思科认证考试。

思科认证考试中心查询网址: <http://www.pearsonvue.com.cn/>

1.3.2 考试登记

到考点填写 Pearson Vue Certification Registration Sheet (Cisco 考生注册表), 预定考试时间 (一般至少要提前两个工作日), 交费 (费用是 250 美金, 约人民币 2000 元左右。如果是思科网络技术学院的学生, 还有机会申请优惠, 优惠后的金额是 250 美金的 3 折, 约人民币 600 元左右)。很多省份和城市并没有 VUE 考试中心, 可以咨询考点, 很多考点都提供了表格网下载, 填完后传真到考试中心, 并从网上银行汇款, 确认考试已经被注册, 这样可以省去一次奔波。

考生考试当天需要提前半个小时到考试中心签到, 并进行生物采集手续。务必要携带两种身份证明文件, 可以接受的身份证明文件是: 第一证件为身份证/驾驶执照/护照; 第二证件为驾驶执照/护照 (不作为第一证件的时候) /学生证/工作证/带本人姓名的信用卡/应届毕业生证 (需要提前三个工作日申请) /劳动保障卡/暂住证。需要提醒的是, 公司人事部门开具的工作证明及户口本, 不能作为第二证件使用, 具体可以咨询考试中心。

1.3.3 考前问卷调查

考试系统为 VUE, 开始是问卷调查, 内容也略有不同。但是不用担心, 全部选 B 相对安全, 因为 B 选项通常表示考生水平一般, 抽取的考题也不会太难。选完一道, 单击“NEXT”按钮继续, 一直到 END。注意: 其中有一个调查是问你是否已满 18 周岁, 一定要选已满 18 周岁。

最后一个调查问是否同意 Cisco 的协议, 这个选项一定要选“同意”, 如果选“不同意”, 那么考试作废, 不同意 Cisco 的协议, 意味着放弃考试。曾经有人选了不同意, 结果就不用考试了。要想再考, 需要再交一次考试费, 重新注册这门考试。

协议过后, 在调查问卷页面右下角单击“END”按钮, 结束问卷调查。考试系统自动开始从服务器抽取题目, 题目一般在前一个工作日已由考试中心从网上下载完毕, 暂存于服务器中。数秒后, 题目抽取完毕, 考生可单击“START”按钮, 开始正式考试。

1.3.4 正式考试

考前问卷填完后, 接下来是正式考试。做完一道题后, 单击“NEXT”按钮, 做下一道题, 切记不可返回上一道题修改, 也就是说, 如果单击了“NEXT”按钮, 将无法返回前一题进行修改, 实在不会做, 建议选择最有把握的答案填入, 不要在一题上耽误过多时间。考试语言为英文, 目前在国内已经有 CCNA 中文版的考试, 但很少有考生参加中文版的考试, 原因主要有三个方面: 一、中文版的考题网上还没有下载; 二、一些考题翻译得不准确, 很容易产生误解; 三、思科的路由器和交换机都是英文的命令行, 学点英文对自己没坏处。共有 55~65 道考题, 中国是 120 分钟考试时间, 1000 分为满分, 849 分通过。如果考前没有经过题海战术, 高水平的工程师也不一定能顺利通过。第一次考试的人可能会紧张, 其实只要准备充分, 考试时间还是足够的, 这一点可以放心。

考试题型有:

(1) **选择题**。单选或多选, 一般是单选还是多选有提示, 或者告诉考生选择所有认为对的答案(也就是所谓的不定选择, 这种题较少出现)。

(2) **实验题**。实验考题对大多数考生来说都比较难, 其实不是考题本身难, 主要原因是多数考生缺乏实验设备, 即所谓的手生。本书会给大家推荐两款路由器和交换机的模拟软件, 可以起到以假乱真的效果, 让读者可以得到充足的动手练习。实验考题分为配置题和排错题。配置题: 让你使用相关命令, 把网络配通, 先在各个路由器上查看命令是否完整, 接下来进行配置, 配置完成后进行检验, 确认无误后保存; 排错题: 实验配置达不到目的, 要求更改配置, 使之满足题目要求。

(3) **拖图题**。给出多个选项, 根据题目要求, 把选项拖到对应的位置。

在考试中也可能会碰到死机现象, 不用紧张, 赶紧告诉监考官, 他们会解决的。重新启动计算机, 继续做题, 以前做的题目结果仍然存在, 只是死机当时正在做的题目可能会没有存上, 一定要仔细检查一下, 再单击“NEXT”按钮继续。

全部题目做完, 单击“END EXAM”按钮, 结束考试。

考试结束, 激动人心的时刻来了, 马上就会看到考试结果。走出考场后, 考官会打印你的成绩单, 盖上钢印。成绩单要保存好, 上面有考生的 ID 号、分数, 还有将来注册时的网址等相关信息。



1.4 CCNA 证书相关内容

通过 CCNA 考试后, 如何取得证书, 以及证书的有效期等还是需要特别关注的。2007 年 8 月 1 日起, Cisco 的考试代理商由 PROMETRIC (普尔文) 换成了 VUE, 考试认证追踪系统也进行了升级, 与过去的系统相比, 现在少了电子证书、快递证书功能。

1.4.1 考后注册

在通过 CCNA 的认证考试后，会立即拿到考试成绩单。但是要取得证书，必须再进行注册，在通过考试的 10 天内，需要到思科官方网站的考生个人跟踪系统中登录个人信息。网址是 <http://www.cisco.com/go/certifications/login/>，如有变动请参考 CCNA 成绩单上的网址。以前很多考生都未重视考后注册，往往造成收不到证书或将来考其他科目无法更改考生个人信息的情况，所以，考试注册最好自己来，密码不要轻易告诉别人。

如果想快一点收到证书，可以在个人信息表中用本国语言写上通信地址。个人信息表通信地址分为三部分，进入后第一部分是由考试中心已经填好的，考生需要检查一下，地址、邮编、E-mail 必须正确无误；第二部分空着不填；第三部分可以用本国语言填上通信地址，和第一部分内容对应即可。注册部分非常关键，建议咨询考官或在有经验的朋友帮助下完成，不要造成不必要的等待或证书的遗失。

注册成功后，等待 6~8 周，思科会把证书按照考生填的地址发过来。证书是按平信的方式邮出，里面包括：一张考生卡片、思科总裁约翰·钱伯斯签发的祝贺信、CCNA 证书。

1.4.2 证书的重发

各个考生的证书处理速度是不一样的，快的从注册完到收到证书只需 2 周，慢的则需 8 周。所以请大家不必着急，时间允许范围是 2 个月，也可以登录网站查询证书状态，网站会显示证书何时被寄出。假如在 2 个月内还没有收到证书，估计就有问题了，可以去向 Cisco 申诉。如果考生的纸质证书没有收到，也可以发邮件到 ciscotraining@external.cisco.com 和 ciscotraining@cisco.com，说明情况，思科会酌情免费发送一次电子版证书。

如果想向思科申请，发出第二张纸质证书或第二份电子版证书，都需要交纳 15 美金，需要存在 VISA 信用卡中，转账完成。详情请网上查阅“如何申请 CCNA 证书重发”。

1.4.3 证书的有效期

CCNA 认证的有效期为三年。如需重新认证，必须通过现有的 CCNA 考试，或者通过 ICND 考试，或者通过 642 专业等级或思科合格专家考试（不包括销售专家考试）中的任何一项，也可以通过现有的 CCIE 笔试。

第 2 章

网络互联和参考模型***

本章主要介绍常见的几种网络分类方法和两种主要的网络参考模型。从人类的通信引入网络通信，介绍两个主要的网络模型 ISO/OSI 和 TCP/IP 参考模型，读者要明白分层的概念，明白相关层的功能和服务，掌握 IP 地址分类和子网划分，了解常见的网络传输介质和网络设备。本章中，读者将获得使用网络工具软件的经验，如 Sniffer，这些工具软件的使用不仅可以帮助读者理解协议的分层，明白数据在网络中的流动，还可以帮助读者在工程中排除网络故障。



2.1 网络的分类**

简单地说，网络就是在一定的区域内将两个或两个以上的计算机以一定的方式连接起来，以供用户共享文件、程序、数据等资源。下面就几种常见的网络类型及分类方法做简单的介绍。

2.1.1 按覆盖范围分*

- **局域网**（Local Area Network, LAN）：局域网一般在几十米到几千米范围内，一个局域网可以容纳几台至几千台计算机。局域网一般具有如下特性：局域网分布在比较小的地理范围内。因为可以采用不同传输能力的传输介质和传输设备，所以局域网的传输距离和传输速度也有差异；局域网往往用于某一群体。比如一个公司、一个单位、某一幢楼、某一个学校等。
- **城域网**（Metropolis Area Network, MAN）：城域网是规模局限在一座城市范围内的区域性网络。城域网的速度比广域网快，符合宽带趋势，因此现在发展很快。与局域网相比，城域网具有分布地理范围广的特点，一般来说，城域网的覆盖范围介于 10~100km 之间。
- **广域网**（Wide Area Network, WAN）：广域网是将分布在各地的局域网络连接起来的网络，是“网间网”（网络之间的网络）。广域网的范围非常大，可以跨越国界、洲界，甚至全球范围。

局域网是组成其他两种类型网络的基础，城域网一般都加入了广域网。广域网的典型代表是 Internet。目前还有两个比较流行的网络概念：存储区域网（Storage Area Network, SAN）和虚拟专用网（Virtual Private Network, VPN）。SAN 是专用的高性能网络，它用于在服务器与存储资源之间传输数据。由于 SAN 是一个独立的专用网络，从而可以避免在客户机与服务器之间的任何传输冲突。VPN 是一种在公共网络上传输私有网络数据的专用网

络技术，利用 VPN，一个远程用户或分支机构可以与总部之间建立一条安全的隧道，用于传输私有数据。本书有专门的章节介绍 VPN 的概念和配置。

2.1.2 按拓扑结构分*

网络拓扑 (Topology) 确定了网络的结构。网络拓扑有两种：一种是物理拓扑，是指实际布线或设备相互连接的几何形式；另一种是逻辑拓扑，它定义了媒体如何存取由主机发送的数据。

1. 物理拓扑

按照物理拓扑结构的不同，可以将网络分为星型网络、环型网络、总线型网络三种基本类型。

(1) **总线型拓扑**。网络中所有的站点共享一条数据通道，总线的两端有端结点，如图 2-1-1 所示。总线型网络安装简单方便，需要铺设的电缆最短，成本低，某个站点的故障一般不会影响整个网络，但介质的故障会导致网络瘫痪。总线网安全性低、监控比较困难、增加新站点也不如星型拓扑网络容易。所以，总线型网络结构现在基本上已经被淘汰。

(2) **环型拓扑**。环型网络结构的各站点通过通信介质连成一个封闭的环形，如图 2-1-2 所示。环形网络容易安装和监控，但容量有限，网络建成后，难以增加新的站点。因此，现在组建局域网已经基本上不使用环型网络结构了。

(3) **星型拓扑**。各站点通过点到点的链路与中心站点相连，如图 2-1-3 所示。星型网络很容易在网络中增加新的站点，数据的安全性和优先级容易控制，易实现网络监控，一个站点出了问题，不会影响整个网络的运行，但中心结点的故障会引起整个网络瘫痪。星型网络结构是现在最常用的网络拓扑结构。

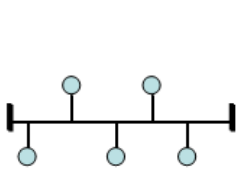


图 2-1-1 总线型拓扑

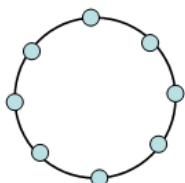


图 2-1-2 环型拓扑



图 2-1-3 星型拓扑

在这三种类型的网络结构基础上，可以组合出扩展星型、层次型、网状型等其他类型拓扑结构的网络，如图 2-1-4 所示。

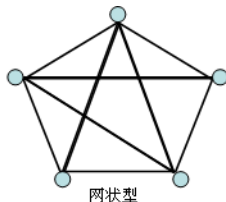
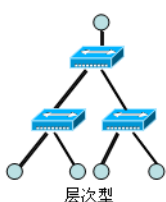
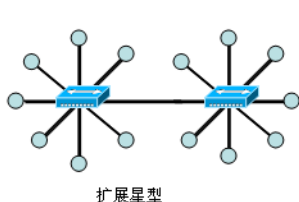


图 2-1-4 其他类型拓扑

2. 逻辑拓扑

网络的逻辑拓扑是指各台主机通过传输介质相互通信的方式。最常见的两种逻辑拓扑

形式是广播拓扑和令牌拓扑。

(1) **广播拓扑**。每台主机都把所要发送数据的目标地址设为网络介质上某个特定网络接口卡的地址、多播地址或广播地址，然后把该数据发送到传输介质中。每台主机使用传输介质时不必遵循某种次序，即先来先服务。现在最常使用的以太网就是采用这种方式来工作的，本书后面有专门的章节来介绍以太网技术。

(2) **令牌拓扑**。令牌拓扑通过向各台主机顺序传递一个电子令牌来控制网络介质的访问。当一台主机接收到令牌时，它就可以把数据发送到网络介质上；如果该主机没有数据要发送，那么就将令牌传递给下一台主机，如此循环。使用令牌传递的主要有令牌环和光纤分布式数据接口（FDDI），它们都是在物理环型拓扑上使用令牌传递的。

2.1.3 按传输介质分***

按照网络的传输介质分类，可以将计算机网络分为有线网络和无线网络两种。有线网络包括采用同轴电缆、双绞线、光纤等有线介质连接的计算机网络。局域网通常采用单一的传输介质，而城域网和广域网采用多种传输介质。

1. 双绞线

采用双绞线连网，因价格便宜，安装方便，所以是目前最常见的连网方式。

(1) 双绞线的类型。计算机局域网中的双绞线可分为非屏蔽双绞线、铝箔屏蔽的双绞线和屏蔽双绞线。

非屏蔽双绞线（Unshielded Twisted Paired, UTP），如图 2-1-5 所示，因价格低廉、容易安装及重新配置，所以是最常见的传输介质，它由两股线规很细的铜线（通常为实心）组成，互相绝缘，以固定间隔彼此绞合在一起，绞合的作用是为抵消电脉冲传输过程中所形成的电磁场。现在，UTP 被广泛用于局域网领域，以便把终端与集线器、交换机和路由器连接起来。在传输距离（理论上是 100m）范围内，五类 UTP 的数据传输速率可以达到 100Mb/s（bit per second，比特每秒），甚至 1000Mb/s。

铝箔屏蔽的双绞线（Foil Twisted Pair, FTP），如图 2-1-6 所示，带宽较大，抗干扰能力强。相对的，屏蔽线比非屏蔽线价格及安装成本要高一些，线缆弯曲性能稍差。六类线及六类之前的屏蔽系统多采用这种形式。

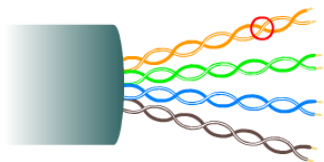


图 2-1-5 非屏蔽双绞线

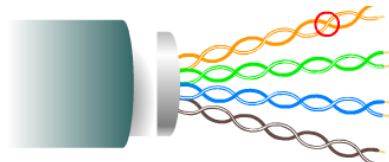


图 2-1-6 铝箔屏蔽的双绞线

屏蔽双绞线（Shielded Twisted-Pair, STP），如图 2-1-7 所示，每一对双绞线都有一个铝箔屏蔽层。四对双绞线合在一起，并且还有一个公共的金属编织屏蔽层，这是七类线的标准结构。它适用于高速网络的应用，提供高度保密的传输，支持未来的新型应用，有助于统一当前网络应用的布线平台，使得从电子邮件到多媒体视频的各种信息，都可以在同一套高速系统中传输。额外的屏蔽层使得七类线有一个较大的线径，这些特点要求在设计安装和端接时要特别小心，要留有很大的空间和较大的弯曲半径。屏蔽双绞线需要一层金属铝箔，即覆盖层把电缆中的每对线包起来，有时候利用另一覆盖层把多对电缆中的各对

线包起来，或利用金属屏蔽层取代这层包在外面的金属铝箔。覆盖层和屏蔽层有助于吸收环境干扰，并将其导入地下以消除这种干扰。这意味着金属铝箔和屏蔽层在焊接时必须与焊接导体时同样小心，而且确保导入地下的机制安全可靠。STP 和 FTP 的成本高得多，而且安装过程难得多。

(2) 双绞线的做法。在讲述双绞线做法之前，先来了解一下水晶头（RJ-45）的引脚。要注意区分 RJ-45 和 RJ-11，RJ-11 只有 4 根针脚，用于电话线接头；而 RJ-45 有 8 根针脚，用于以太网连接。RJ-11 连接器在形状上明显小于 RJ-45 连接器。

RJ-45 水晶头包括两端，一端是插头，另一端是插孔。插头可以接入计算机、集线器、交换机或路由器的以太网接口上，而插孔和连接导线（现在最常用的是非屏蔽双绞线的五类线）相连。EIA/TIA（电子工业协会“EIA”和电信工业协会“TIA”开发了一个叫做 EIA/TIA-568 商用建筑布线标准的商业建筑电信布线标准）制定的布线标准规定了不同颜色的 4 对双绞线与针脚连接。EIA/TIA-568 标准规定了两种连接标准，即 EIA/TIA-568A 和 EIA/TIA-568B，两种标准并没有实质上的差别。将 RJ-45 的插头端面对眼睛，并使带有 8 个铜质接触点的一面在下方，那么最左边是 ①，最右边是 ⑧，如图 2-1-8 所示。

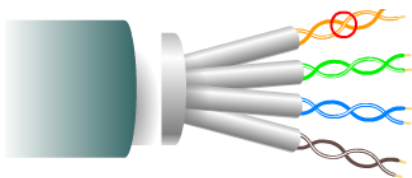


图 2-1-7 独立屏蔽双绞线

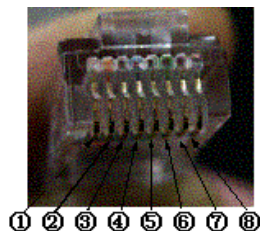


图 2-1-8 RJ-45 引脚编号

T568A 规定的连接方法是：

- ①——绿 - 白（就是白色的外层上有些绿色，表示和绿色的是一对线）
- ②——绿色
- ③——橙 - 白（就是白色的外层上有些橙色，表示和橙色的是一对线）
- ④——蓝色
- ⑤——蓝 - 白（就是白色的外层上有些蓝色，表示和蓝色的是一对线）
- ⑥——橙色
- ⑦——棕 - 白（就是白色的外层上有些棕色，表示和棕色的是一对线）
- ⑧——棕色

T568B 规定的连接方法是：

- ①——橙 - 白
- ②——橙色
- ③——绿 - 白
- ④——蓝色
- ⑤——蓝 - 白
- ⑥——绿色
- ⑦——棕 - 白
- ⑧——棕色

在 10Mb/s 和 100Mb/s 以太网中只使用两对导线。也就是说，只使用 4 根针脚。标准规定使用的 4 根针脚是 1、2、3 和 6，1 和 2 用于发送，3 和 6 用于接收，如表 2-1-1 所示。

表 2-1-1 RJ-45 引脚作用表

针脚编号	作 用
针脚 1	发送+
针脚 2	发送-
针脚 3	接收+
针脚 4	不使用
针脚 5	不使用
针脚 6	接收-
针脚 7	不使用
针脚 8	不使用

目前，中国普遍使用的是 T568B 标准。这里特别要强调一下，线序是不能随意改动的。例如，从上面的连接标准来看，1 和 2 是一对线，而 3 和 6 又是一对线。但如果将以上规定的线序弄乱，例如，将 1 和 3 用做发送的一对线，而将 2 和 6 用做接收的一对线，那么这些连接导线的抗干扰能力就要下降，误码率就可能增大，这样就不能保证以太网的正常工作了。

根据应用场合不同，双绞线有 3 种类型：直通线、交叉线和全反线。

- **直通线**（Straight-through）。双绞线两端接入 RJ-45（水晶头）的线序相同，国内多采用的是 T568B。这种线主要用于不同种设备的互连，比如计算机—交换机、计算机—集线器、交换机—路由器等。这里要特别强调的是，计算机和路由器属于同一种设备，集线器和交换机属于同一种设备，也就是说，计算机和路由器间、集线器和交换机间不能使用直通的双绞线相连，因为它们是同种设备。
- **交叉线**（Crossover）。双绞线两端接入 RJ-45 的线序不同，一端保持 T568B 的线序，另一端使用 T568A 标准（也就是把 T568B 标准中 1 和 3、2 和 6 互换）。有人可能会奇怪，双绞线中有 8 根，为何只交叉其中的 4 根呀？双绞线虽然有 8 根，但在要求不高的情况下，真正用于数据传输的只有 1、2、3、6 这 4 根线，剩下 4、5、7、8 这 4 根线主要起到屏蔽等辅助作用。这也是我们经常发现有些工程中只有一根双绞线接入，计算机和电话却可以同时使用，这是因为施工人员为图方便，偷工减料，把双绞线中不用的 4 根挪用出 2 根给了电话。交叉线主要用于同种设备的互连，比如计算机—计算机、路由器—路由器、集线器—集线器。尤其值得注意的是，“计算机—路由器”也使用交叉线，因为路由器和计算机的硬件组成几乎完全相同，可以用计算机来充当路由器，Windows Server 2000/2003/2008 还支持多种动态路由协议，另外，“集线器—交换机”也用此种线缆。同种设备接口卡的引脚作用相同，如果使用直通线把同种设备连接起来，将出现两端都是发送端或都是接收端，数据传输失败。
- **全反线**（Rollover）。全反线两端接入 RJ-45 的线序完全相反，这种线主要用于对路由器和交换机进行初始配置之用，有时也用于异步传输。

值得注意的是，随着技术的发展，现在有些新款交换机或路由器能自动识别所接设备的类型，并调整接口状态，自动适应线缆的类型。但在 CCNA 考试中，默认没有使用支持智能接口的设备，一定要满足同种设备使用交叉线、不同设备使用直通线的要求。

2. 同轴电缆

如图 2-1-9 所示,与双绞线相比,同轴电缆含有线规较粗的单层实心导体,导体一般由铜或覆以铜的铝制成。中间的导体外面覆以一层绝缘材料,这种绝缘材料有助于把中间的导体和外面的金属铝箔屏蔽层隔开。外面通常会包一层金属网,再包一层保护皮对电缆加以保护。中间粗粗的导体可支持高频信号,几乎不会出现困扰 UTP 及其同类电缆的信号衰减问题。

以太网及其他 LAN 技术原先使用同轴电缆是因为它能支持高频信号,而且不受电磁干扰影响。然而,面对迅猛发展的双绞线,成本高昂加上安装困难导致同轴电缆退居其后。现在使用同轴电缆较多的网络是有线电视网。

同轴电缆根据粗细程度不同,分为粗缆(10Base5)和细缆(10Base2),粗缆的传输距离是 500m,细缆的传输距离是 185m。

3. 光纤网

光导纤维简称光纤,光纤传输距离长,传输速率高,可达数千兆 bps,抗干扰性强,不会受到电子监听设备的监听,是高安全性网络的理想选择。光纤是细如头发般的透明玻璃丝,可用来传导光信号。光纤由纤芯和包层组成,由于纤芯的折射率大于包层的折射率,故光波在界面上形成全反射,使光只能在纤芯中传播,实现通信。

工程中使用最多的分法是按光纤横截面上折射率来分,有单模光纤和多模光纤。单模光纤纤芯直径较小,采用激光作为光源,传输的方向是沿光纤直径方向,如图 2-1-10 所示,因此单模光纤数据传输速率较快,传输距离较远,价格相对较贵;多模光纤纤芯直径较大,采用发光二极管作为光源,传输的方向是全反射,如图 2-1-10 所示,因此多模光纤数据传输速率较慢,传输距离较近,价格相对较便宜。

4. 无线网

无线网采用微波、红外线、无线电等传输,由于无线网络的连网方式灵活方便,是一种很有前途的组网方式。本书有专门的章节介绍无线组网。



图 2-1-9 同轴电缆

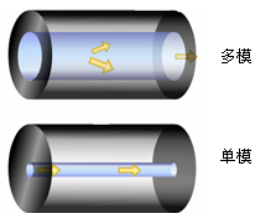


图 2-1-10 光在多模和单模光纤中的传输方向

2.1.4 按服务方式分*

按照网络的服务方式分类,可以将计算机网络分为客户机/服务器网和对等网两种。

1. 客户机/服务器 (Client/Server) 网

服务器是指专门提供服务的高性能计算机或专用设备,客户机是指用户计算机。这是客户机向服务器发出请求并获得服务的一种网络形式,多台客户机可以共享服务器提供的各种资源。这是最常用、最重要的一种网络类型。不仅适合于同类计算机联网,也适合于

不同类型的计算机联网,如 PC、Mac 机的混合联网。这种网络安全性容易得到保证,计算机的权限、优先级易于控制,监控容易实现,网络管理能够规范化。网络性能在很大程度上取决于服务器的性能和客户机的数量。目前针对这类网络有很多优化性能的服务器,称为专用服务器。

2. 对等网 (Peer-to-Peer)

对等网不要求专用服务器,每台客户机都可以与其他客户机对话,共享彼此的信息资源和硬件资源,组网的计算机一般类型相同。这种网络方式灵活方便,但是较难实现集中管理与监控,安全性也低,较适合于部门内部协同工作的小型网络。

另外还有一些非正规的分类方法,如企业网、校园网,根据名称便可理解。从不同的角度对网络有不同的分类方法,每种网络名称都有特殊的含义。了解网络的分类方法和类型特征,是熟悉网络技术的重要基础之一。



2.2 网络体系结构

1969 年 12 月, DARPA 的计算机分组交换网 ARPANET 投入运行。ARPANET 的成功,标志着计算机网络的发展进入了一个新纪元。ARPANET 的成功运行使计算机网络的概念发生了根本性的变化。早期的面向终端的计算机网络是以单个主机为中心的星型网,各终端通过传输介质共享主机的硬件和软件资源。但分组交换网则以通信子网为中心,主机和终端都处在网络的边缘。主机和终端构成了用户资源子网,用户不仅共享通信子网的资源,而且还可共享用户资源子网的丰富的硬件和软件资源。这种以通信子网为中心的计算机网络通常被称为第二代计算机网络。

在第二代计算机网络中,多台计算机通过通信子网构成一个有机的整体,既分散又统一,从而使整个系统性能大大提高。原来单一主机的负载可以分散到全网的各个计算机上,使得网络系统的响应速度加快,而且在这种系统中,单机故障也不会导致整个网络系统的全面瘫痪。在网络中,相互通信的计算机必须高度协调工作,而这种“协调”是相当复杂的。为了降低网络设计的复杂性,早在当初设计 ARPANET 时就有专家提出了层次模型。分层设计方法可以将庞大而复杂的问题转化为若干较小且易于处理的子问题。

有了网络体系结构,使得一个公司所生产的各种机器和网络设备可以非常容易被连接起来。但由于各个公司的网络体系结构各不相同,所以不同公司之间的网络不能互连互通。针对上述情况,国际标准化组织(International Standard Organization, ISO)于 1977 年设立专门的机构研究解决上述问题,并于不久后提出了一个使各种计算机能够互连的标准框架——开放式系统互连参考模型(Open System Interconnection/Reference Model, OSI/RM),简称 OSI。OSI 模型是一个开放体系结构,它规定将网络分为 7 层,并规定每层的功能。OSI 参考模型的出现,意味着计算机网络发展到第三代。在 OSI 参考模型推出后,网络的发展道路一直走标准化道路,而网络标准化的最大体现就是 Internet 的飞速发展。现在 Internet 已成为世界上最大的国际性计算机互联网。Internet 遵循 TCP/IP 参考模型,由于 TCP/IP 仍然使用分层模型,因此 Internet 仍属于第三代计算机网络。如今,计算机网络从体系结构到实用技术已逐步走向系统化、科学化和工程化。

要想让两台计算机进行通信,必须使它们采用相同的信息交换规则。我们把在计算机网络中用于规定信息的格式,以及如何发送和接收信息的一套规则称为网络协议(Network

Protocol) 或通信协议 (Communication Protocol)。为了减少网络协议设计的复杂性, 网络设计者并不是设计一个单一、巨大的协议来为所有形式的通信规定完整的细节, 而是采用把通信问题划分为许多个小问题, 然后为每个小问题设计一个单独的协议的方法。这样做使得每个协议的设计、分析、编码和测试都比较容易, 正如我们编程一样, 通过编写“过程”和“函数”以方便调用, 来把一个复杂的程序模块化、简单化、独立化。分层模型是一种用于开发网络协议的设计方法。本质上, 分层模型描述了把通信问题分为几个小问题 (称为层次) 的方法, 每个小问题对应于一层。

为了减少网络设计的复杂性, 绝大多数网络采用分层设计方法。所谓分层设计方法, 就是按照信息的流动过程将网络的整体功能分解为一个个的功能层, 不同机器上的同等功能层之间采用相同的协议, 同一机器上的相邻功能层之间通过接口进行信息传递。

为了便于理解接口和协议的概念, 下面以邮政通信系统为例进行说明。人们平常写信时, 都有个约定, 这就是信件的格式和内容。首先, 写信时必须采用双方都懂的语言文字和文体, 开头是对方称谓, 最后是落款等。这样, 对方收到信后, 才可以看懂信中的内容, 知道是谁写的、什么时候写的等。信写好之后, 必须将信封封装并交给邮局寄发, 这样寄信人和邮局之间也要有约定, 这就是规定信封写法并贴邮票。在中国寄信必须先写收信人的地址和姓名, 然后再写寄信人的地址和姓名。邮局收到信后, 首先进行信件的分拣和分类, 然后交付有关运输部门进行运输, 如航空信交民航、平信交铁路运输或公路运输等。这时, 邮局和运输部门也有约定, 如到站地点、时间、包裹形式等。信件运送到目的地后进行相反的过程, 最终将信件送到收信人手中, 收信人依照约定的格式才能读懂信件。如图 2-2-1 所示, 在整个过程中, 主要涉及了 3 个子系统, 即用户子系统、邮政子系统和运输子系统。

从上例可以看出, 各种约定都是为了达到将信件从一个源点送到某一个目的点这个目标而设计的, 这就是说, 它们是因信息的流动而产生的。可以将这些约定分为同等机构间的约定, 如用户之间的约定、邮政局之间的约定和运输部门之间的约定, 以及不同机构间的约定, 如用户与邮政局之间的约定、邮政局与运输部门之间的约定。

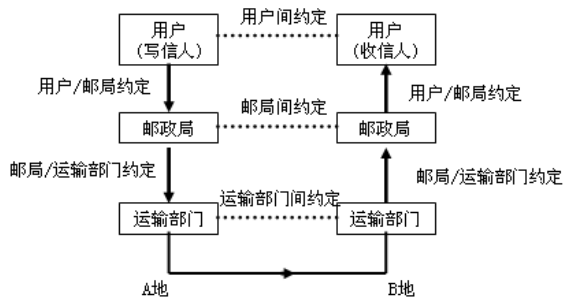


图 2-2-1 邮政系统分层模型

的约定, 如用户与邮政局之间的约定、邮政局与运输部门之间的约定。虽然两个用户、两个邮政局、两个运输部门分处甲、乙两地, 但它们都分别对应同等机构, 同属一个子系统, 譬如两地的邮政局同属于邮政子系统; 而同处一地的不同机构则不在一个子系统内, 譬如邮政局和运输部门, 它们之间的关系是服务与被服务的关系。很显然, 这两种约定是不同的, 前者 (两个邮政局) 为部门内部的约定, 而后者 (邮政局和运输部门) 是不同部门之间的约定。在计算机网络环境中, 两台计算机中的两个进程之间进行通信的过程与邮政通信的过程十分相似。

为了减少计算机网络设计的复杂性, 人们往往按功能将计算机网络划分为多个不同的功能层。网络中同等层之间的通信规则就是该层使用的协议, 如有关第 N 层的通信规则的集合, 就是第 N 层的协议。而同一计算机的不同功能层之间的通信规则称为接口 (Interface), 在第 N 层和第 $(N+1)$ 层之间的接口称为 $N/(N+1)$ 层接口。总的来说, 协议是不同机器同等层之间的通信约定, 而接口是同一机器相邻层之间的通信约定。不同的网络, 分层数量、

各层的名称和功能，以及协议都各不相同。然而，在所有的网络中，每一层的目的都是向它的上一层提供一定的服务。

协议层次化不同于程序设计中模块化的概念。在程序设计中，各模块可以相互独立，任意拼装或者并行，而层次则一定有上下之分，它是依数据流的流动而产生的。组成不同计算机同等层的实体称为对等进程。对等进程不一定必须是相同的程序，但其功能必须完全一致，且采用相同的协议。

分层设计方法将整个网络通信功能划分为垂直的层次集合后，在通信过程中，下层将向上层隐蔽下层的实现细节，但层次的划分应首先确定层次的集合及每层应完成的任务。划分时应按逻辑功能组合，并具有足够的层次，以使每层小到易于处理。同时层次也不能太多，以免产生难以负担的处理开销。

计算机网络体系结构是网络中分层模型及各层功能的精确定义。对网络体系结构的描述必须包括足够的信息，使实现者可以为每一功能层进行硬件设计或编写程序，并使之符合相关协议。但我们要注意的，网络协议实现的细节不属于网络体系结构的内容，因为它们隐含在机器内部，对外部来说是不可见的。



2.3 ISO/OSI 参考模型***

前一节讨论了协议分层和网络体系结构，本节将分析和讨论一个重要的网络体系结构，即 ISO/OSI 参考模型。在网络发展的初期，许多研究机构、计算机厂商和公司都大力发展计算机网络。从 ARPANET 出现至今，已经推出了许多商品化的网络系统。这种自行发展的网络，在体系结构上差异很大，以至于它们之间互不相容，难以相互连接以构成更大的网络系统。为此，许多标准化组织和委员会积极开展了网络体系结构标准化方面的工作，包括：国际标准化组织（ISO）、电气和电子工程师协会（IEEE）、美国国家标准学会（ANSI）、国际电信联盟（ITU）、电子工业联盟/电信工业协会（EIA/TIA）等。其中最为著名的就是国际标准化组织（ISO）提出的开放系统互连参考模型（OSI）。OSI 参考模型是研究如何把开放式系统（即为了与其他系统通信而相互开放的系统）连接起来的标准，该模型的最大作用就是促成了不同厂商之间的协同工作。

OSI 参考模型将计算机网络分为 7 层，如图 2-3-1 所示。本节将从最低层开始，依次讨论模型的各层所要完成的功能。

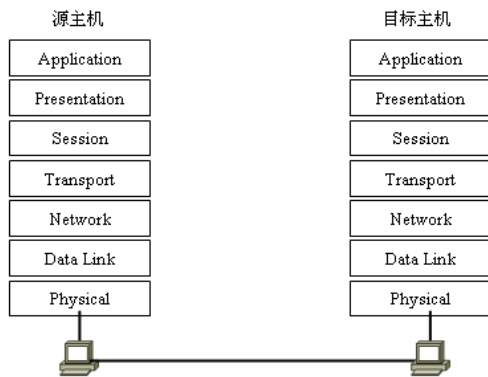


图 2-3-1 OSI 七层模型

2.3.1 物理层***

1. 物理层（Physical Layer）的功能

物理层的主要功能是完成相邻结点之间原始比特流的传输，控制数据怎样被放置到通信介质上。物理层协议关心的典型问题是使用什么样的物理信号来表示数据“1”和“0”；一位持续的时间多长；数据传输是否可同时在两个方向上进行；最初的连接如何建立和完成，通信后连接如何终止；物理接口（插头和插座）有多少针以及各针的用处等。物理层的设计主要涉及物理层接口的机械、电气、功能和过程特性，以及物理层接口连接的传输介质等问题，物理层的设计还涉及通信工程领域内的一些问题。

2. 物理层的主要网络设备

（1）中继器（Repeater）

中继器是连接网络线路的一种装置，常用于两个网络结点之间物理信号的双向转发工作。中继器是最简单的网络互联设备，主要完成物理层的功能，负责在两个结点的物理层上按位传递信息，完成信号的复制、调整和放大功能，以此来延长网络的长度。由于存在损耗，在线路上传输的信号功率会逐渐衰减，衰减到一定程度时将造成信号失真，因此会导致接收错误。中继器就是为解决这一问题而设计的，它完成物理线路的连接，对衰减的信号进行放大，保持与原数据相同。一般情况下，中继器的两端连接的是相同的媒体，但有的中继器也可以完成不同媒体的转接工作。从理论上讲中继器的使用是无限的，网络也因此可以无限延长。事实上这是不可能的，因为网络标准中都对信号的延迟范围作了具体的规定，中继器只能在此规定范围内进行有效的工作，否则会引起网络故障。

前面介绍过双绞线理论上的最大传输距离是 100m，如果超过 100m，由于信号的衰减，很难保证信息传输的正确性，可以使用中继器来延长传输的距离。中继器仅适用于以太网，可将两段或两段以上（使用多个中继器）的以太网互连起来。

（2）集线器（Hub）

集线器相当于多端口的中继器，也可以把信号整形、放大后发送到所有结点上。我们知道在环型网络中只存在一个物理信号传输通道，都是通过一条传输介质来传输的，这样就存在各结点争抢信道的矛盾，传输效率较低。引入集线器这一网络设备后，每一个工作站是用它自己专用的传输介质连接到集线器的，各结点间不再只有一个传输通道，各结点发回来的信号通过集线器集中，集线器再把信号整形、放大后发送到所有结点上，这样至少在上行通道上不再出现碰撞现象。但基于集线器的网络仍然是一个共享介质的局域网，这里的“共享”其实就是集线器内部总线，所以当上行通道与下行通道同时发送数据时仍然会存在信号碰撞现象。当集线器在其内部端口检测到碰撞时，产生碰撞强化信号向集线器所连接的所有端口进行传送。这时所有数据都将不能发送成功。我们可以用一个形象的现实情形来说明，那就是单车道上同时有两个方向的车驶来。我们知道，单车道上通常只允许一个行驶方向的车通过，但是在小城镇，条件有限通常没有这样的规定，单车道也有可能允许两个行驶方向的车通过，但是必须是不同时刻经过。在集线器中也一样，虽然各结点与集线器的连接已有各自独立的通道，但是在集线器内部却只有一个共同的通道，上、下行数据都必须通过这个共享通道发送和接收数据，这样有可能像单车道一样，当上、下行通道同时有数据发送时，就可能出现塞车现象。

正因为集线器的这一不足之处，所以它不能单独应用于较大网络中（通常是与交换机等设备一起分担小部分的网络通信负荷），就像在大城市中心不能有单车道一样，因为网络越大，出现网络碰撞现象的机会就越大。也正因如此，集线器的数据传输效率是比较低的，因为它在同一时刻只能有一个方向的数据传输，也就是所谓的“半双工”方式。生活中最常见的使用“半双工”方式工作的设备有对讲机，按下通话键时，可以讲话，但不能接听；松开通话键，可以接听，但不能说话。生活中的电话采用的是“双工”工作方式，可以同时说话和听话；而收音机采用的则是“单工”方式，永远只能是接听，单方向传输。如果网络中要选用集线器作为单一的连接设备，那么网络的规模最好在 10 台以内，而且集线器带宽应为 10/100Mb/s 以上。

集线器除了共享带宽这一不足之处外，还有另一个方面的不足必须要考虑，那就是它的广播工作方式。因为集线器属于 OSI 七层模型的物理层，基本上不具有“智能”的能力，更别说“学习”功能了。它也不具备交换机所具有的 MAC 地址表，所以它发送数据时都是没有针对性的，而是采用广播方式发送。也就是说，当它要向某结点发送数据时，不是直接把数据发送到目的结点，而是把数据包发送到与集线器相连的所有结点。如图 2-3-2 所示，源主机 PC-A 需要发送数据到目的主机 PC-B，PC-A 把数据包发往集线器，集线器从端口 1 收到数据包后，然后把该数据包复制，并把信号放大后从端口 2、3、4 发送出去，尽管 PC-C 和 PC-D 不是目的主机，它们也会收到 PC-A 给 PC-B 发的数据包。

这里引入两个概念：冲突域（Collision Domain）和广播域（Broadcast Domain）。当两个比特在同一介质上同时传输时就会产生冲突。所谓冲突域就是指发送数据给一个单一目标（也就是单播帧，第 3 章中会解释什么样的帧是单播帧）所影响的范围，如图 2-3-2 中，PC-A 发送数据到目的主机 PC-B，结果集线器将把该数据包转发到除接收端口以外的所有端口，PC-C 和 PC-D 也收到了该数据，它们属于同一个冲突域；所谓广播域是指发送数据给一个不明确目标（也就是广播帧或组播帧，第 3 章中会解释什么样的帧是广播帧或组播帧）所影响的范围，如图 2-3-2 中，PC-A 发送一个广播包，集线器将把该广播包转发到除接收端口以外的所有端口，集线器上的所有设备属于同一个广播域。结论：所有通过集线器（不管有多少个集线器）互连的网络中只有一个广播域、一个冲突域。

这种广播式发送数据有两方面的不足：第一，用户数据包向所有结点发送，很可能带来数据通信的不安全因素，一些别有用心的人很容易就能截获他人的数据包；第二，由于所有数据包都是向所有结点同时发送，加之以上所介绍的共享带宽方式，就更加可能造成网络拥塞现象，降低网络执行效率。

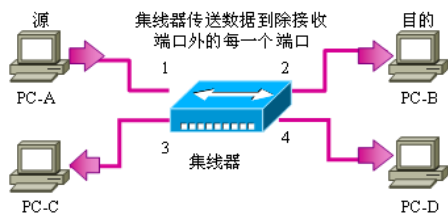


图 2-3-2 集线器的工作原理

2.3.2 数据链路层***

1. 数据链路层（Data Link Layer）的功能

数据链路层的主要功能是如何在不可靠的物理线路上进行数据的可靠传输。数据链路层完成的是网络中相邻结点之间可靠的数据通信。为了保证数据的可靠传输，发送方把用户数据封装成帧（Frame），并按顺序传送各帧。由于物理线路的不可靠，因此发送方发出的数据帧有可能在线路上出错或丢失，从而导致接收方不能正确接收到数据帧。为了保证能让接收方对接收到的数据进行正确性判断，发送方为每个数据分块计算出 CRC（循环冗余

余检验），并把 CRC 添加到帧中，这样接收方就可以通过重新计算 CRC 来判断数据接收的正确性。一旦接收方发现接收到的数据有错，则发送方必须重传这一帧数据。然而，相同帧的多次传送也可能使接收方收到重复的帧。比如，接收方给发送方的“确认帧”被破坏后，发送方也会重传上一帧，此时接收方就可能接收到重复帧。数据链路层必须解决由于帧的损坏、丢失和重复所带来的问题。

数据链路层要解决的另一个问题是防止高速发送方的数据把低速接收方“淹没”。因此，需要某种信息流量控制机制使发送方得知接收方当前还有多少缓存空间。为了控制的方便，流量控制常常和差错处理一同实现。

2. 数据链路层的主要网络设备

在最普遍的以太网中，数据链路层通过 MAC（Media Access Control，媒体访问控制）地址负责主机之间数据的可靠传输。数据链路层的设备必须能够识别出数据链路层的地址，即 MAC 地址。一个设备如果能识别 MAC 地址，该设备至少是数据链路层以上的设备。数据链路层的网络设备主要有网卡、网桥和交换机。

(1) 网卡（NIC）

网卡（Network Interface Card，NIC）也叫网络适配器，是连接计算机与网络的硬件设备，网卡的主要工作原理是整理计算机上发往网线上的数据，并将数据分解为适当大小的数据包之后向网络上发送出去。对于网卡而言，每块网卡都有一个唯一的网络结点地址，它是网卡生产厂家在生产时烧入 ROM（Read Only Memory，只读存储芯片）中的，我们把它叫做 MAC 地址，且保证绝对不会重复。可以人为地修改 MAC 地址的显示（有些网卡提供的驱动程序可以修改 MAC 地址，也有些工具可以修改 MAC 地址，但并没有更改 ROM 中的内容，只是修改了 MAC 的显示，当计算机重新安装操作系统后，MAC 地址还是出厂时的 MAC 地址）。

网卡插在计算机或服务器扩展槽中，通过网络线（如双绞线、同轴电缆或光纤）与网络交换数据、共享资源。计算机对接收到的数据帧进行比较，如果数据帧中的目标 MAC 地址与本机网卡的 MAC 地址相同，或者目标 MAC 地址是广播 MAC 地址，即“FFFFFFFF”，则计算机对数据帧进行处理；否则，计算机丢弃该数据帧。

可以在 DOS 窗口中使用“ipconfig /all”命令查看计算机网卡的 MAC 地址，如图 2-3-3 所示，网卡的 MAC 地址是“00-1B-24-7D-25-72”，用十六进制表示，占用 48 个比特，前 24 个比特表示厂商，后 24 个比特为设备编号，。

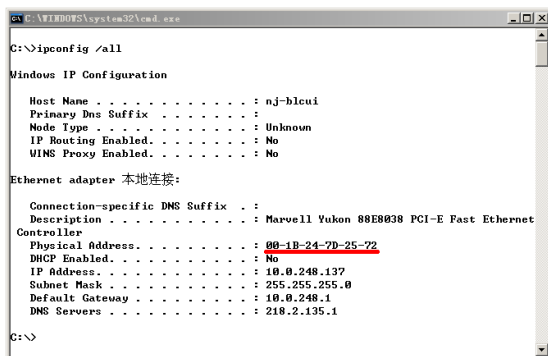


图 2-3-3 查看网卡的 MAC 地址

(2) 网桥 (Bridge)

网桥工作在数据链路层，用于将两个 LAN 连接在一起并按 MAC 地址转发帧。物理层的集线器可以扩展网络的规模，但所有通过集线器相连的主机属于同一个冲突域，任何时刻只能有一台主机发送数据，如果有两台主机同时发送数据就会发生冲突，导致数据发送失败。当同一个冲突域中的主机数据量非常多时，数据发生冲突的可能性大大增加，此时可以使用网桥来分隔冲突域。网桥可以用来分隔冲突域，把一个冲突域分隔成两个冲突域，通过增加冲突域的数量，减小每个冲突域的大小，减少冲突发生的可能。连接两个网段的网桥能从一个网段向另一个网段传送完整而且正确的帧，不会传送干扰或有问题的帧。

网桥主要用于互联以太网分段，传输需在两个不同分段间传输的信息，但是阻断局部分段内的信息，因此网桥减少了网络上的通信总量。

在图 2-3-4 中包括 2 台集线器、4 台计算机、1 台网桥。每个网桥保存一个动态的 MAC 地址表，这个表通常称为 CAM (Content Addressable Memory，内容可寻址存储器)，由站点的 MAC 地址和网桥的端口号组成。初始时，该 MAC 地址表为空，以后通过学习方法获取 MAC 地址信息。当一个数据帧到达网桥时，网桥根据其源 MAC 地址以及到达的端口号，向 MAC 地址表中增加或刷新一条记录。

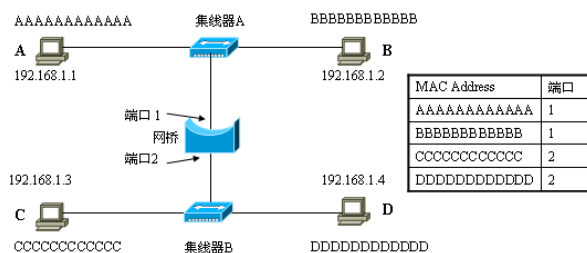


图 2-3-4 网桥工作方式图

网桥的工作过程如下：

① 刚加电时，网桥的 MAC 地址表是空的，假使计算机 A (192.168.1.1) 要发送数据给计算机 B (192.168.1.2)，计算机 A 对数据包进行封装（假设计算机 A 已经知道计算机 B 的 MAC 地址，在 2.4.2 节会介绍计算机 A 如何获得计算机 B 的 MAC 地址），把数据包发送到集线器 A，集线器 A 把数据包发往除接收端口以外的所有端口（计算机 B 和网桥）。

② 网桥收到这个数据包后，首先在 MAC 地址表中添加这个数据帧的源 MAC 地址，即计算机 A 的 MAC 地址“AAAAAAAAAAAA”和对应的端口 1，然后网桥在自己的 MAC 地址表中查找这个数据帧中的目的 MAC 地址，即“BBBBBBBBBBBB”，结果没有找到，网桥把这个数据包从端口 2 转发出去。从网桥端口转发出来的数据包到达集线器 B，集线器 B 把这个数据包从除接收到端口以外的端口转发出去，计算机 C 和计算机 D 收到这个数据包并进行检查，结果发现这个数据帧中的目的 MAC 地址与自己网卡的 MAC 地址不同，计算机 C 和计算机 D 丢弃这个数据包。

③ 集线器 A 也把数据包转发到计算机 B，计算机 B 收到这个数据包并检查数据包中的目的 MAC 地址，发现与自己的 MAC 地址相同，计算机 B 接收这个数据包，并对计算机 A 进行确认。计算机 B 封装数据包后发往集线器 A，数据帧的源 MAC 地址是“BBBBBBBBBBBB”，目的 MAC 地址是“AAAAAAAAAAAA”，集线器 A 把数据包发往除接收端口以外的所有端口（计算机 A 和网桥）。

④ 网桥收到这个数据包后，首先在 MAC 地址表中添加这个数据帧的源 MAC 地址，即计算机 B 的 MAC 地址和对应的端口 1，然后网桥在自己的 MAC 地址表中查找这个数据帧中的目的 MAC 地址，即“AAAAAAAAAAAA”，结果发现该数据帧的源和目的 MAC 地址在网桥的同一个端口上，即端口 1，网桥不再转发该数据帧到端口 2。

⑤ 最后，网桥会学到所有 MAC 地址和端口的对应，如图 2-3-4 中的表所示，表中记录了计算机 A 和计算机 B 在网桥的端口 1，计算机 C 和计算机 D 在网桥的端口 2。此后，计算机 A 与计算机 B、计算机 C 与计算机 D 可以同时通信，相互不受影响。

同中继器一样，网桥也是连接两个网段的设备。但和中继器不同之处在于，网桥侦听每个网段上的信号，当它从一个网段接收到一个帧时，网桥会检查并确认该数据帧是否已经完整地到达，然后，如果需要的话就把该数据帧传送到其他网段。这样，两个 LAN 网段通过网桥连接后，就像一个 LAN 一样，网中任何一台计算机可发送数据帧到任何其他计算机。因为每个网段都支持标准的网络连接并使用标准的帧格式，计算机并不知道它们是连接在同一 LAN 网段中还是连接在一个桥接网中。

因为网桥能检查出一些故障，所以比中继器使用更广泛。两个通过中继器相连的网段，如果由于闪电而导致其中一个网段上有电干扰，中继器会把它传送到另一个网段。相反，如果干扰发生在通过网桥连接的网段中，网桥接收到一个不正确的帧，丢弃该帧。类似地，网桥不会把从一个网段传送来的冲突信号传送到另一个网段。因此，网桥会把故障控制在一个网段中而不会影响到另一个网段。图 2-3-4 中计算机 A 和计算机 B 是一个冲突域，计算机 C 和计算机 D 是另一个冲突域。因网桥转发广播或组播帧，所以 4 台计算机在同一个广播域中。网桥比中继器和集线器对数据包做更多的处理，延时也相对增加，一个 2 端口的网桥包括两个冲突域、一个广播域。

(3) 交换机 (Switch)

与网桥的工作过程类似，交换机也根据源 MAC 学习，根据目的 MAC 进行转发，按每一个数据帧中的 MAC 地址决策信息转发。在图 2-3-5 中，交换机也会学到并维护表中的 MAC 地址表，当源主机“AAAAAAAAAAAA”发送一个数据帧给目的主机“BBBBBBBBBBBB”时，交换机收到这个数据帧，查找交换机的 MAC 地址表，发现目的 MAC 地址在交换机的端口 2，交换机从端口 2 把数据帧转发出去，端口 3 和端口 4 不受影响。

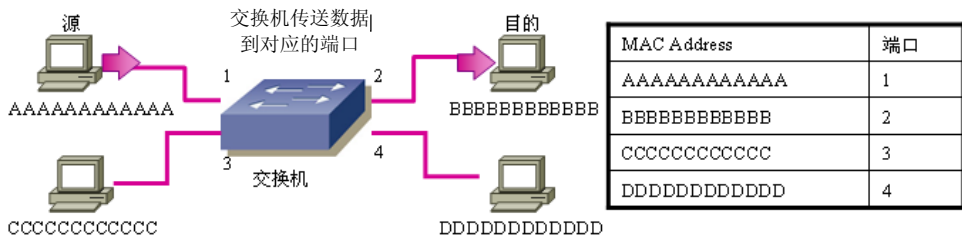


图 2-3-5 交换机的转发过程

CCNA 考试中经常涉及交换机转发方式的考题，交换机转发方式分为 3 种情况：情况一，交换机对已知的单播帧，只往对应的端口转发；情况二，交换机对未知的单播帧，即交换机还没有学到数据帧中的目的 MAC 地址，交换机泛洪数据包，即发往除接收端口以外的所有端口；情况三，交换机对组播帧和广播帧进行泛洪转发，即发往除接收端口以外的所有端口。有关交换机转发方式的讲解和演示请观看光盘中的视频文件“视频\2-1.wrf”。

类似于网桥，交换机提供了网络互联功能。交换机的每个端口都是一个独立的冲突域，可以为每个工作站提供更高的带宽。因为交换机可以使用现有的电缆、中继器、集线器和工作站的网卡，不必做高层的硬件升级；交换机对工作站是透明的，这样管理开销低廉，简化了网络结点的增加、移动和网络变化的操作；并且交换机的价格与集线器所差无几，所以在当今的网络中，交换机被普遍使用。

可以简单地把交换机看成是多端口的网桥，但二者还是有一些区别的：首先，网桥一般只有 2 个端口，而一般交换机最少也有 4 个端口，还有 24 端口、48 端口，甚至更多口的交换机；其次，网桥采用软件进行转发，而交换机采用专门设计的集成电路，基于硬件进行数据转发，交换机以线路速率在所有的端口并行转发信息，提供了比传统网桥高得多的操作性能，操作接近单个局域网性能，远远超过了普通网桥互联网络之间的转发性能；最后，交换机的端口造价远低于网桥。

根据功能不同，交换机可分为：

① **传统的二层交换机**，与集线器相比，仅仅多了 MAC 地址表的功能。属于 OSI 七层模型的数据链路层，有一个广播域（传统的二层交换机转发广播或组播帧到除接收端口以外的所有端口）、多个冲突域（每个端口就是一个冲突域）。

② **VLAN（Virtual Local Area Network，虚拟局域网）型交换机**，可网管型交换机，比传统型交换机多了 VLAN 的功能。它仍属于数据链路层，有多个广播域（每个 VLAN 就是一个广播域）、多个冲突域（每个端口就是一个冲突域），并可配置 IP 地址，方便远程管理。

③ **三层交换机**，比 VLAN 型交换机多了路由功能，可以把三层交换机想象成路由器 + VLAN 型交换机，但三层交换机的数据包转发性能要比路由器 + VLAN 型交换机的性能高出许多倍。它属于 OSI 七层模型的网络层，具有多个广播域、多个冲突域。工程中出于安全的考虑，有时需要把 IP 和 MAC 进行绑定，这就需要三层及三层以上的交换机才能完成，因为普通的二层交换机处在 OSI 七层模型的第二层，识别不了三层的 IP 地址，也就无法完成绑定。

有关交换机的更多介绍和配置，请参阅本书的 9~12 章。

2.3.3 网络层***

网络层（Network）的主要功能是完成网络中主机间的报文传输。在广域网中，这包括产生从源端到目的端的路由，根据采用的路由协议，选择最优的路径，本书将在后面章节介绍路由的相关知识。

网络层涉及的协议有 IP、IPX 等，网络层的设备必须能识别出网络层的地址，比如路由器、三层交换机等都可以根据 IP 地址做路径选择，它们都属于网络层设备。

路由器是一种连接多个网络或网段的网络层设备，它能将不同网络或网段之间的数据进行“翻译”，以使它们能够相互“读懂”对方的数据，从而构成一个更大的网络。它不是应用于同一网段的设备，而是应用于不同网段或不同网络之间的设备。路由器之所以能在不同网络之间起到“翻译”的作用，是因为它不再是一个纯硬件设备，而是支持相当丰富路由协议的软、硬结合的设备，支持的协议有 RIP、OSPF、EIGRP 等，这些路由协议就是用来实现连通不同网段或网络的。

路由器有两大典型功能，即数据通道功能和控制功能。数据通道功能包括转发决定、

背板转发, 以及输出链路调度等, 一般由特定的硬件来完成; 控制功能一般用软件来实现, 包括与相邻路由器之间的信息交换、系统配置、系统管理等。

路由器具有判断网络地址和选择路径的功能, 它能在多网络互联环境中, 建立灵活的连接, 可用完全不同的数据分组和介质访问方法连接各种子网。路由器属于网络层的一种互联设备, 有隔离广播的作用, 它的每个端口都是一个单独的广播域, 也是一个单独的冲突域。

在局域网接入广域网的众多方式中, 通过路由器接入互联网是最为普遍的方式。使用路由器互联网络的最大优点是: 各互联子网仍保持各自独立, 每个子网可以采用不同的拓扑结构、传输介质和网络协议, 网络结构层次分明。通过路由器与互联网相连, 则可完全屏蔽公司内部网络, 有些路由器内部还集成了入侵防御和防火墙功能, 因此使用路由器可以用来防御攻击, 保护内部网络的安全。

路由器和交换机的比较如表 2-3-1 所示。

表 2-3-1 路由器和交换机的比较

特 点	路 由 器	交 换 机
数据转发速度	慢	快
OSI 层	第三层	第二层
使用的地址	逻辑地址——IP	物理地址——MAC
广播	阻止	转发
安全性	较高	较低

2.3.4 传输层***

传输层 (Transport Layer) 是整个网络的关键部分, 实现两个用户进程间端到端 (End-to-End) 的可靠通信, 处理数据包错误、数据包次序, 以及其他一些关键传输问题。向下提供通信服务的最高层, 弥补通信子网的差异和不足, 向上是用户功能的最低层。与数据链路层有相似之处, 不同的地方在于前者是端到端的, 后者是点到点的, 而且比数据链路层协议复杂得多。

传输层的主要功能有: 提供建立、维护和拆除传输层连接, 向网络层提供合适的服务, 提供端到端的错误恢复和流量控制, 向会话层提供独立于网络层的传送服务和可靠的透明数据传输。

传输层相关的协议有 TCP (Transmission Control Protocol, 传输控制协议)、UDP (User Datagram Protocol, 用户数据报协议), 它们涉及服务使用的端口号, 主机根据端口号识别服务 (常用的 WWW 服务端口号是 80, Telnet 服务端口号是 23 等), 区分会话 (源 IP、源端口号、目标 IP、目标端口号, 四者共同唯一标识一个会话)。对一些常用的服务, 在文件 “C:\WINDOWS\system32\drivers\etc\services” 中记录了服务名、所使用的协议 (TCP 或 UDP)、默认端口号等。

这里介绍一种识别不同应用所使用服务端口的方法, 譬如查看 Windows 中 “远程桌面” 服务所使用的服务端口。假如在计算机 “10.0.248.137” 上, 使用远程桌面登录到计算机 “210.28.203.187”, 然后在被控制的远程计算机上执行 “netstat -n” 命令 (当然也可以在本地上计算机上执行这个命令), 如图 2-3-6 所示, 可以看到远程主机上使用的是 “3389” 端口, 这就是 Windows 远程桌面使用的默认端口。采用类似的方法, 可以获知其他应用所使用的

端口号。



图 2-3-6 查看应用程序的端口号

有关 TCP 和 UDP 协议，本书在后面的 TCP/IP 参考模型中再详述。

2.3.5 会话层***

会话层（Session Layer）允许不同机器上的用户之间建立会话关系，会话层提供的服务之一是管理对话控制。会话层允许信息同时双向传输，或任一时刻只能单向传输。如果属于后者，类似于物理信道上的半双工模式，会话层将记录此时该轮到哪一方。一种与对话控制有关的服务是令牌管理，有些协议保证双方不能同时进行同样的操作，这一点很重要。为了管理这些活动，会话层提供了令牌，令牌可以在会话双方之间移动，只有持有令牌的一方可以执行某种关键性操作。另一种会话层服务是同步，如果在平均每小时出现一次大故障的网络上，两台机器间要进行一次两小时的文件传输，想想会出现什么样的问题？每一次传输中途失败后，都不得不重新传送这个文件。当网络再次出现大故障时，可能又会半途而废。为了解决这个问题，会话层提供了一种方法，即在数据中插入同步点。每次网络出现故障后，仅仅重传最后一个同步点以后的数据。

CCNA 考试中几乎不涉及会话层。

2.3.6 表示层***

表示层（Presentation Layer）完成某些特定的功能，对这些功能人们常常希望找到普遍的解决办法，而不必由每个用户自己来实现。值得一提的是，表示层以下各层只关心从源主机到目标主机可靠地传送比特，而表示层关心的是所传送的信息的语法和语义。表示层服务的一个典型例子是用一种大家一致选定的标准方法对数据进行编码。

网络上计算机可能采用不同的数据表示，所以需要在数据传输时进行数据格式的转换。例如在不同的机器上常用不同的代码来表示字符串（ASCII 和 EBCDIC）、整型数（二进制反码或补码），以及机器字的不同字节顺序等。为了让采用不同数据表示法的计算机之间能够相互通信并交换数据，我们在通信过程中使用抽象的数据结构来表示传送的数据，而在机器内部仍然采用各自的标准编码。管理这些抽象数据结构，并在发送方将机器的内部编码转换为适合网上传输的传送语法，以及在接收方做相反的转换等，都是由表示层来完成的。

此外，表示层还涉及数据压缩和解压、数据加密和解密等工作。

2.3.7 应用层***

联网的目的在于支持运行于不同计算机上的进程进行通信，而这些进程则是为用户完成不同任务而设计的。可能的应用是多方面的，不受网络结构的限制。应用层（Application Layer）包含大量人们普遍需要的协议，如 HTTP（Hyper text Transfer Protocol，超文本传输

协议),这个大家并不陌生,该应用默认使用的是 TCP 的 80 端口;FTP(File Transfer Protocol, 文件传输协议),多用于因特网上的文件传输,该应用管理端口默认使用的是 TCP 的 21 号端口,另外,FTP 服务还要使用到数据端口,数据端口因 FTP 的主动和被动模式有异,这里不再深入讨论;SMTP(Simple Mail Transfer Protocol,简单邮件传输协议),用于邮件的发送,该应用默认使用的是 TCP 的 25 号端口;POP3(Post Office Protocol Version 3,邮局协议版本 3),用于邮件的接收,该应用默认使用的是 TCP 的 110 号端口;DNS(Domain Name System,域名系统),用于因特网上域名的解析,譬如把南京大学的域名“www.nju.edu.cn”解析成 IP 地址“202.119.32.7”,该应用默认使用的是 UDP 和 TCP 的 53 号端口;Telnet(远程登录),Telnet 是一种字符模式的终端服务,它可以使用户通过网络进入远程主机或网络设备,然后对远程主机或网络设备进行操作,这种连通可以发生在局域网里面,也可以通过互联网进行,该应用默认使用的是 TCP 的 23 号端口。这里列出的一些常用应用都是需要考生了解的,感兴趣的读者可以架设相关的服务器,毕竟大家的生活中经常要使用这些服务。

对于需要通信的不同应用来说,应用层的协议都是必需的。比如,当某个用户想要获得远程计算机上的一个文件拷贝时,他要向本机的文件传输软件发出请求,这个软件与远程计算机上的文件传输进程通过文件传输协议进行通信,这个协议主要处理文件名、用户许可状态和其他请求细节的通信。远程计算机上的文件传输进程使用其他特征来传输文件内容。

由于每个应用有不同的要求,应用层的协议集在 ISO/OSI 模型中并没有定义,但是,有些确定的应用层协议,包括虚拟终端、文件传输和电子邮件等都可作为标准化的候选。值得注意的是,OSI 模型本身不是网络体系结构的全部内容,这是因为它并未确切地描述用于各层的协议和实现方法,而仅仅告诉我们每一层应该完成的功能。不过,ISO 已经为各层制定了相应的标准,但这些标准并不是模型的一部分,它们是作为独立的国际标准被发布的。

OSI 参考模型是在其协议开发之前设计出来的,这意味着 OSI 模型不是基于某个特定的协议集而设计的,因而它更具有通用性。但另一方面,也意味着 OSI 模型在协议实现方面存在某些不足。实际上,OSI 协议过于复杂,这也是 OSI 从未真正流行开来的原因所在。

虽然 OSI 模型和协议并未获得巨大的成功,但是 OSI 参考模型在计算机网络的发展过程中仍然起到了非常重要的指导作用,作为一种参考模型和完整体系,它仍对今后计算机网络技术朝标准化、规范化方向发展具有指导意义。接下来看看目前被广泛使用的 TCP/IP(Transmission Control Protocol/Internet Protocol,传输控制协议/网际协议)协议。



2.4 TCP/IP 参考模型***

TCP/IP 是目前最成功、使用最频繁的互联网协议。本节介绍 TCP/IP 参考模型,以及 ARP、RARP、ICMP、TCP 和 UDP 等协议。

TCP/IP 参考模型是四层结构,下面结合 Sniffer 软件来讲解 TCP/IP 参考模型的四层结构。Sniffer 软件是 NAI 公司推出的功能强大的协议分析软件,具有捕获网络流量进行详细分析、实时监控网络活动、利用专家分析系统诊断问题、收集网络利用率和错误等功能。Sniffer 的工作方式就是通过将网卡置为混杂模式,对网卡上接收到的数据包进行侦听、捕获和分析。有关 Sniffer 软件的安装和简单使用请参考光盘中“补充资料\附录 2 Sniffer

软件的安装”文件。如图 2-4-1 所示是 Sniffer 软件捕获的 DNS 查询和应答包。

在图 2-4-1 中，可以看到一个完整的 TCP/IP 应用数据包分为四层，分别是网络访问层（Network Access），也就是图 2-4-1 中的“DLC”层，包括 OSI 模型的物理层和数据链路层，在这一层可以看到数据帧的源和目的 MAC 地址；网际层（Internet），也就是图 2-4-1 中的“IP”层，相当于 OSI 模型中的网络层，在这一层可以看到数据包的源和目的 IP 地址；传输层（Transport），也就是图 2-4-1 中的“UDP”层，和 OSI 模型中的传输层一致，在这一层可以看到数据分段源和目的端口，以及所使用的协议，从图中可以看出，DNS 服务主要使用的是 UDP 协议，服务端口是 53；应用层（Application），也就是图 2-4-1 中的“DNS”层，包括 OSI 模型的上三层，即会话层、表示层和应用层，应用层中可以看到该 DNS 包是查询“www.nju.edu.cn”域名对应的 IP 地址。

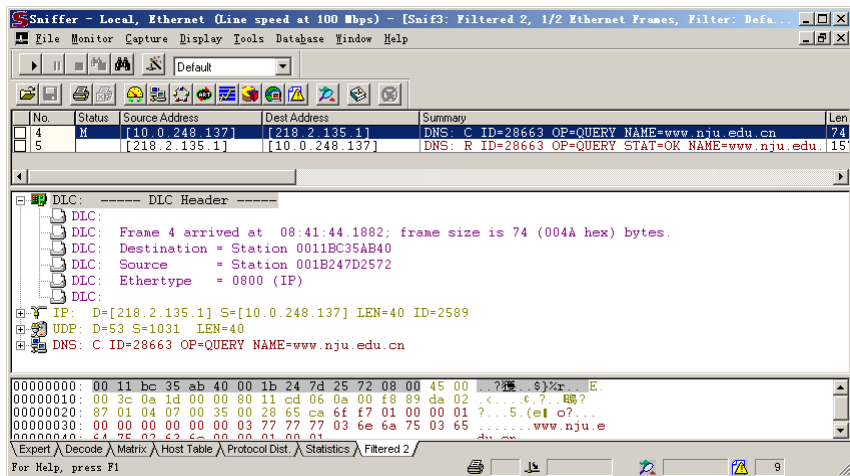


图 2-4-1 TCP/IP 四层模型

ISO/OSI 参考模型是在其协议被开发之前设计出来的。这意味着 ISO/OSI 模型并不是基于某个特定的协议集而设计的，因而它更具有通用性。但另一方面，也意味着 ISO/OSI 模型在协议实现方面存在某些不足。而 TCP/IP 模型正好相反。先有协议，模型只是现有协议的描述，因而协议与模型非常吻合。问题在于 TCP/IP 模型不适合其他协议栈。因此，它在描述其他非 TCP/IP 网络时用处不大。下面来看看两种模型的具体差异。其中显而易见的差异是两种模型的层数不一样：ISO/OSI 模型有七层，而 TCP/IP 模型只有四层。两者都有传输层和应用层，但其他层是不同的。两种模型之间的对应关系如图 2-4-2 所示。

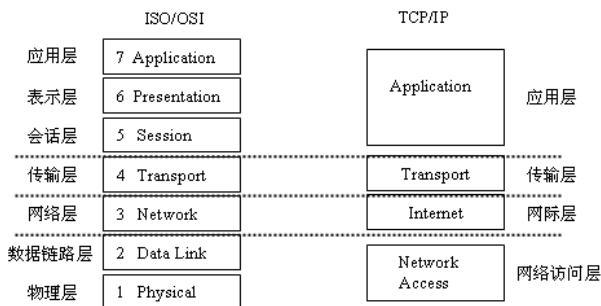


图 2-4-2 两种模型之间的对应关系

2.4.1 网络访问层***

网络访问层（Network Access）的功能包括 IP 地址与物理硬件地址的映射，以及将 IP 分组封装成帧。基于不同硬件类型的网络接口，网络访问层定义了和物理介质的连接。网络访问层包含了数据链路层的地址，如用在以太网上就是 MAC 地址，在图 2-4-1 中，可以看到数据帧的源 MAC 地址、目的 MAC 地址。此层是 TCP/IP 模型的最低层，负责接收从 IP 层传来的 IP 数据报，并将 IP 数据报通过低层物理网络发送出去，或者从低层物理网络上接收物理帧，解封装出 IP 数据报，交给 IP 层处理。

2.4.2 网际层***

网际层（Internet）的主要功能包括三个方面：

- **第一，处理来自传输层的分组发送请求：**将分组装入 IP 数据报，填充报头，选择去往目的结点的路径，然后将数据报发往适当的网络接口。
- **第二，处理输入数据报：**首先检查数据报的合法性，然后进行路由选择，假如该数据报已到达目的结点（本机），则去掉报头，将 IP 报文的数据部分交给相应的传输层协议；假如该数据报尚未到达目的结点，则转发该数据报。
- **第三，处理 ICMP（Internet Control Message Protocol，网际控制信息协议）报文：**即处理网络的路由选择、流量控制和拥塞控制等问题。

TCP/IP 网络模型的互联网层在功能上非常类似于 ISO/OSI 参考模型中的网络层。

网际层上的协议如下：

1. IP 协议

IP 的责任就是把数据从源传送到目的地。它不负责保证传送可靠性、流控制、包顺序和其他对于主机到主机协议来说很普通的服务。IP 实现两个基本功能：寻址和分段。IP 可以根据数据报报头中包括的目的地址将数据报传送到目的地址，在此过程中 IP 负责选择传送的路线，这种选择路线称为路由功能。如果有些网络内只能传送小数据报，IP 可以将数据报重新组装并在报头域内注明。

构成 IP 报头的字段如图 2-4-3 所示，括号中的数值表示该字段所占用的比特数。其中优先级和服务类型字段一般用于 QoS（Quality of Service，服务质量）；存活期（Time To Live，TTL）是数据报可以生存的时间上限，它由发送者设置，每经过一次路由，TTL 至少减 1，如果未到达目的地时生存时间减为零，则抛弃此数据报；源和目的 IP 地址用于表示数据从哪里来，要到哪里去。参加 CCNA 考试的考生没有必要记住 IP 报头中的每一个字段，简单了解上述几个字段就可以了。

版本(4)	报头长度(4)	优先级和服务类型(8)	数据包总长度(16)
标识(16)			标志和偏移量(16)
存活期(8)	协议(8)		报头检验和(16)
源IP地址(32)			
目的IP地址(32)			
选项(0或32)			
数据(可变)			

图 2-4-3 IP 报头格式

IP 不提供可靠的传输服务，它不提供端到端的或结点到结点的确认，对数据没有差错控制，它只使用报头的校验码，不提供重发和流量控制。如果出错可以通过 ICMP 报告，ICMP 在 IP 模块中实现。

2. ICMP (Internet Control Message Protocol, Internet 控制消息协议)

提起 ICMP，一些人可能会感到陌生，实际上，ICMP 与我们息息相关。它是 TCP/IP 协议族的一个子协议，用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

在网络体系结构的各层次中，都需要控制，而不同的层次有不同的分工和控制内容，IP 层的控制功能是最复杂的，主要负责差错控制、拥塞控制等，任何控制都是建立在信息的基础之上的，在基于 IP 数据报的网络体系中，IP 协议自身没有内在机制来获取差错信息并处理。为了处理这些错误，TCP/IP 设计了 ICMP 协议，当某个网关发现传输错误时，立即向信源主机发送 ICMP 报文，报告出错信息，让信源主机采取相应处理措施，它是一种差错和控制报文协议，不仅用于传输差错报文，还传输控制报文。

我们在网络中经常会使用到 ICMP 协议，只不过觉察不到而已。比如经常使用的用于检查网络通不通的 Ping 命令，这个“Ping”的过程实际上就是 ICMP 协议工作的过程。发送主机首先发送一个 ICMP Echo Request 的包，包含 64 字节的数据，它被发送后，接收方会返回一个 ICMP Echo Reply 的包，返回的数据中包含了接收到的数据的拷贝。还有其他的网络命令，如跟踪路由的 Tracert 命令也是基于 ICMP 协议的。

ICMP 报文包含在 IP 数据报中，属于 IP 的一个用户，IP 头部就在 ICMP 报文的前面，所以一个 ICMP 报文包括 IP 头部、ICMP 头部和 ICMP 报文，IP 头部的 Protocol 值为 1 就说明这是一个 ICMP 报文，ICMP 头部中的类型 (Type) 域用于说明 ICMP 报文的作用及格式，此外还有一个代码 (Code) 域用于详细说明某种 ICMP 报文的类型，所有数据都在 ICMP 头部后面。RFC 定义了 13 种 ICMP 报文格式，具体如表 2-4-1 所示。

表 2-4-1 ICMP 报文格式

类型代码	类型描述
0	响应应答 (ECHO-REPLY)
3	不可到达
4	源抑制
5	重定向
8	响应请求 (ECHO-REQUEST)
11	超时
12	参数失灵
13	时间戳请求
14	时间戳应答
15	信息请求 (*已作废)
16	信息应答 (*已作废)
17	地址掩码请求
18	地址掩码应答

其中代码为 15、16 的信息报文已经作废。下面是几种常见的 ICMP 报文。

- **响应请求。**我们日常使用最多的 ping，就是响应请求（Type=8）和应答（Type=0），一台主机向一个结点发送一个 Type=8 的 ICMP 报文，如果途中没有异常（例如被路由器丢弃、目标不回应 ICMP 或传输失败），则目标返回 Type=0 的 ICMP 报文，说明这台主机存在，更详细的 tracert 通过计算 ICMP 报文通过的结点来确定主机与目标之间的网络距离。
- **目标不可到达、源抑制和超时报文。**这三种报文的格式是一样的，目标不可到达报文（Type=3）在路由器或主机不能传递数据报时使用，例如要连接对方一个不存在的系统端口（端口号小于 1024）时，将返回 Type=3、Code=3 的 ICMP 报文，它提示的意思就是目标不可到达。常见的不可到达类型还有网络不可到达（Code=0）、主机不可到达（Code=1）、协议不可到达（Code=2）等。源抑制则充当一个控制流量的角色，它通知主机减少数据报流量，由于 ICMP 没有恢复传输的报文，所以只要停止该报文，主机就会逐渐恢复传输速率。最后，无连接方式网络的问题就是数据报会丢失，或者长时间在网络游荡而找不到目标，或者拥塞导致主机在规定时间内无法重组数据报分段，这时就要触发 ICMP 超时报文的产生。超时报文的代码域有两种取值：Code=0 表示传输超时，Code=1 表示重组分段超时。
- **时间戳。**时间戳请求报文（Type=13）和时间戳应答报文（Type=14）用于测试两台主机之间数据报来回一次的传输时间。传输时，主机填充原始时间戳，接收方收到请求后填充接收时间戳后以 Type=14 的报文格式返回，发送方计算这个时间差。

3. ARP（Address Resolution Protocol，地址解析协议）

ARP 负责将某个 IP 地址解析成对应的 MAC 地址。在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的 MAC 地址的。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的 MAC 地址。但这个目标 MAC 地址是如何获得的呢？它就是通过地址解析协议获得的，所谓“地址解析”就是主机在发送帧前根据目标 IP 地址得出目标 MAC 地址的过程。ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。

结合图 2-4-4，讲解 ARP 的工作过程如下：

① 计算机 A 欲发送数据包到计算机 B，计算机 A 确定要访问的计算机 B 与本计算机处在同一个网络 192.168.1.0 中，计算机 A 在本机的缓存中查询计算机 B 的 IP 地址所对应的 MAC 地址。

② 如果计算机 A 在本地缓存中找到 192.168.1.3 对应的 MAC 地址，则计算机 A 用此 MAC 地址封装帧，并发送出去。

③ 如果计算机 A 在本地缓存中没有找到 192.168.1.3 对应的 MAC 地址，则计算机 A 发送一个 ARP 的查询包（ARP Request）。ARP 查询包中的源 IP 地址是计算机 A 的 IP 地址 192.168.1.2，目标 IP 地址是计算机 B 的 IP 地址 192.168.1.3，源 MAC 地址是计算机 A 的 MAC 地址 00-1B-24-7D-25-02，ARP 查询包中的目的 MAC 地址是广播 MAC 地址 FF-FF-FF-FF-FF-FF。计算机 A 封装完成后，把 ARP 查询包以广播的形式发送出去。

④ 计算机 B 和计算机 C 均收到此广播包，计算机 B 和计算机 C 解封装该数据包，计算机 B 和计算机 C 发现数据帧中的目的 MAC 不是本机网卡的 MAC 地址，但是广播 MAC 地址，计算机 B 和计算机 C 解封装该数据帧，把数据包传到网络层。计算机 C 检查数据包

的目的 IP 地址,发现目的 IP 地址是 192.168.1.3,与本机不同,计算机 C 放弃继续处理该数据包,同时在本地的缓存中增加或更新 192.168.1.2 对应的 MAC 地址条目。计算机 B 检查数据包中的目的 IP 地址,发现目的 IP 地址是 192.168.1.3,与本机相同,计算机 B 在本地的缓存中增加或更新 192.168.1.2 对应的 MAC 地址条目。

⑤ 计算机 B 发现 ARP 查询包是询问本机 IP 地址所对应的 MAC 地址的,计算机 B 将发回 ARP 应答包 (ARP Reply)。ARP 应答包的源 IP 地址是 192.168.1.3,目的 IP 地址是 192.168.1.2,源 MAC 地址是 00-1B-24-7D-25-03,目的 MAC 地址是 00-1B-24-7D-25-02。该 ARP 应答包以单播的方式发送出去。

⑥ 如果是集线器相连的网络,则计算机 A 和计算机 C 均会收到此 ARP 应答包;如果是交换机相连的网络,因交换机可以基于目的 MAC 地址转发,则只有计算机 A 可以收到此 ARP 应答包。计算机 C 比较数据帧的目的 MAC 地址,发现与本机的不同,计算机 C 丢弃该数据包。计算机 A 收到此 ARP 应答包,可以获得计算机 B 对应的 MAC 地址。

⑦ 计算机 A 获得计算机 B 的 MAC 地址后,计算机 A 就可以向计算机 B 发送其他数据了。

从上面的讲解中可知,ARP 请求包是广播包,而 ARP 应答包是单播包。读者朋友如果想获知同一个局域网中某台计算机的 MAC 地址,可以先 ping 一下该计算机的 IP 地址,然后使用“arp -a”命令可以查看本机的 ARP 缓存表,从中可以找到某个 IP 地址对应的 MAC 地址。读者还可以使用“arp -d”命令删除本机的 ARP 缓存,使用“arp -s”命令把 IP 地址和 MAC 地址进行绑定。

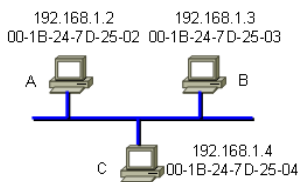


图 2-4-4 ARP 工作过程

有关 ARP 工作原理和报文格式的讲解和演示请观看光盘中的视频文件“视频\2-1.wrf”。

注意: 如果一台主机需要访问远端主机,数据帧封装的目的 MAC 地址并不是远端主机的 MAC 地址,而是网关的 MAC 地址,有关这一点,本章后面有专门的讲解。

4. Proxy ARP (代理 ARP)

前面介绍的 ARP 协议可以帮助主机或路由器获知局域以太网上某个 IP 地址对应的 MAC 地址,可却无法获知一台远程主机对应的 IP 地址,因为 ARP 查询包是广播包,路由器有隔离广播的作用,致使 ARP 查询包无法穿越路由器而到达远端的目的主机。局域网内的主机可以配置默认网关来访问远端主机,可主机不允许配置多个默认网关,考虑一下,如果某个默认网关(一般是路由器)因故障停机,会怎么样呢?即使该局域网还有另一台出口路由器,主机也不会向其他的路由器发送数据,此时需要重新配置主机的网关。而代理 ARP 则可以在这种情况下自动帮助那些在某个子网中的主机,在不重新配置路由甚至默认网关的情况下,发送数据到远端主机。

使用代理 ARP 可以在网络中单独增加一台路由器,而不会影响其他路由器的路由表。但是使用代理 ARP 也带来严重不足:使用代理 ARP 将会明显增加网络分段中的传输业务量,并且网络中的主机也将会保持比正常时大许多的 ARP 表,并以此来处理全部的 IP 到 MAC 的地址映射。有关这一点,可以在启用代理 ARP 网段的主机上使用“arp -a”命令查看,会发现有很多非本地子网中 IP 地址的映射条目,在没有启用代理 ARP 的情况下,主机只会有本地子网中主机的 ARP 缓存。

默认时, 所有 Cisco 路由器以太网接口上都启用了代理 ARP, 如果不打算使用它, 可以在路由器接口下使用 “no ip proxy-arp” 命令来关闭该功能。有关代理 ARP 的使用, 请参考光盘中的视频文件 “视频\5-1.wrf”。

5. RARP (Reverse Address Resolution Protocol, 反向地址转换协议)

前面介绍的 ARP 是已知其他计算机的 IP 地址, 查询其他计算机的 MAC 地址。而 RARP 是已知本机的 MAC 地址, 询问本机的 IP 地址。典型用在无盘工作站上, 当一台无盘工作站启动时, 它没有办法在其初始化时了解自己的 IP 地址, 但是, 它可以知道自己的 MAC 地址。无盘工作站可以通过发送 RARP 的包来询问与此 MAC 地址相对应的 IP 地址, 网络上会指定一个被称为 RARP 服务器的计算机来响应这个请求, 这样无盘工作站就会得到自己的 IP 地址。

RARP 是早期提供的通过硬件地址获取 IP 的解决方案, 但它有自身的局限性, 比如 RARP 客户与 RARP 服务器不在同一网段, 中间有路由器等设备连接, 这时候利用 RARP 就显得无能为力, 因为 RARP 请求报文不能通过路由器。BOOTP (Bootstrap Protocol, 引导协议) 协议提供了很好的解决方法, 同样, 在今天的大中型网络中, DHCP (Dynamic Host Configuration Protocol, 动态主机配置协议) 协议也是常用协议之一。接下来对 BOOTP 和 DHCP 进行简单介绍。

BOOTP: BOOTP 也是一种客户/服务器的协议, 可以为无盘操作系统或配置成动态获取的计算机提供 IP 地址、子网掩码、网关 (路由器地址), 以及 DNS 信息。实现过程分两种情况:

- **情况一:** 这与 RARP 工作环境一样, 即客户与服务器在同一网段, BOOTP 服务器被动打开 UDP 端口 67, 客户端通过 UDP 端口 68 发送请求, 因为客户端不知道自己的 IP 地址, 也不知道服务器的 IP 地址, 客户机使用全 0 的源地址与全 1 的目标地址, 服务器通过单播或广播方式响应。
- **情况二:** 客户与服务器在不同网段, 实现的方法是, 每个网段中设置一个中继代理, 中继代理知道服务器的地址, 其收到目标端口为 67 的广播报文, 就将该报文封装成单播数据报, 然后发送给 BOOTP 服务器, 服务器知道该报文来自于中继代理, 因为在中继代理发送的报文中有其 IP 地址, 中继代理收到 BOOTP 服务器的回应后, 把它发送给 BOOTP 请求客户。

DHCP: DHCP 与 BOOTP 协议差不多, 但 DHCP 功能更强, 不仅可以通过租期方便地实现动态分配, 而且还可以提供除 IP 地址、子网掩码、网关, 以及 DNS 以外的几十个网络参数。

ARP、Proxy ARP 和 RARP 也属于网络访问层, 可以说 ARP 协议跨越 OSI 七层模型的二层和三层。正因为如此, 一些处在网络层的防火墙对低层的 ARP 攻击显得无能为力。

2.4.3 传输层***

在 TCP/IP 网络中, IP 采用无连接的数据报机制, 对数据进行 “尽力而为的传递”, 即只管将报文尽力传送到目的主机, 无论传输正确与否, 不做验证, 不发确认, 也不保证报文的顺序。TCP/IP 的可靠性体现在传输层, 传输层协议之一的 TCP 协议提供面向连接的服务 (传输层的另一个协议 UDP 是无连接的)。传输层的主要功能是可靠而又准确地传输并

控制源主机与目的主机之间的信息流，提供端到端的控制，通过滑动窗口机制提供流控制，通过序列号和确认机制来保证可靠性。TCP 传输控制协议发送数据分段时，可以保证数据的完整性。流控制可以避免发送数据的主机使接收主机的缓存溢出的问题，缓存溢出会导致数据的丢失。可靠的传输可以通过下列方法实现：

- 接收方对收到的数据分段向发送方进行确认；
- 发送方向接收方重传所有未被确认的数据分段；
- 在目的端将数据分段按正确的顺序重组，并删除重复的数据分段；
- 提供避免和控制拥塞的机制。

1. TCP

TCP（Transmission Control Protocol，传输控制协议）是一种面向连接的传输层协议，能提供可靠的数据传输。在面向连接的环境中，开始传输数据之前，端点之间先要建立连接。TCP 负责将消息拆分成数据分段，重传丢失的数据分段并将数据分段在目的主机重组成消息。TCP 的数据分段格式如图 2-4-5 所示，参加 CCNA 考试的考生没有必要了解每一个字段，但了解 TCP 报头中的源端口、目的端口、序列号、确认号和窗口，有助于理解 TCP 传输的可靠性和 TCP 的滑动窗口机制。

TCP/IP 协议组常用的协议如图 2-4-6 所示，其中使用 TCP 的应用层协议有 FTP、HTTP、SMTP、POP3、Telnet 和 DNS 等，使用 UDP 的协议有 DNS 和 TFTP 等。

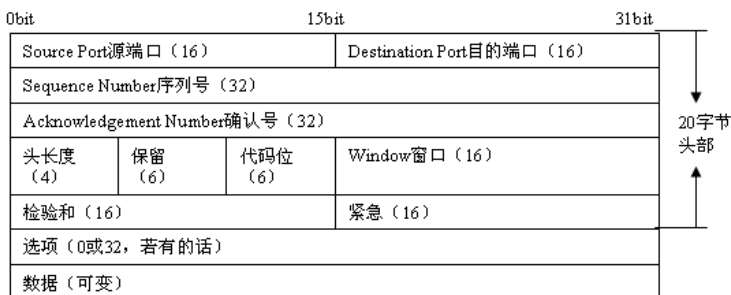


图 2-4-5 TCP 的数据分段格式

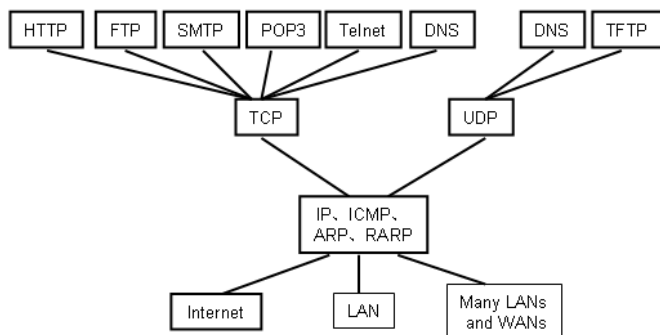


图 2-4-6 TCP/IP 协议组常用协议

2. UDP

UDP (User Datagram Protocol, 用户数据报协议) 是 TCP/IP 协议栈中无连接的传输协议，

其数据分段格式如图 2-4-7 所示。UDP 是一种简单协议，它交换数据报而没有确认机制或传输保证，错误处理和重传机制必须由上层协议来完成。从 TCP 和 UDP 的数据分段格式中可以看出，UDP 的简单性非常明显。UDP 协议主要面向请求/应答式的交易型应用，一次交易往往只有一来一回两次报文交换，假如为此而建立连接和撤销连接，开销是相当大的，这种情况下使用 UDP 就非常有效。另外，UDP 协议也应用于那些对可靠性要求不高，但要求网络的延迟较小的场合，如话音和视频数据的传送。



图 2-4-7 UDP 的数据分段格式

组播一般使用的都是 UDP 协议，很多广播教学软件，譬如“极域电子教室”教学软件等使用的就是组播地址和 UDP 协议，教师机只需要发送一份数据到组播地址，所有的学生机加入这个组播地址，接收教师机的广播教学，学生机的多少对教师机的性能影响不大。

Netmeeting 程序又称网络会议，也可以用于广播教学，教师机可以共享自己的屏幕，可是这款软件使用的是 TCP 协议，是端到端的连接，需要确认重传机制，教师机的性能受学生机数量多少的影响，教师机最多只可以直接连接十几台学生机。

3. 三次握手

TCP 协议是面向连接的，所以它在开始传输数据之前需要先建立连接。要建立或初始化一个连接，两端主机必须同步双方的初始序号。同步是通过交换连接建立数据分段和初始序号来完成的，在连接建立数据分段中包含一个 SYN（同步）的控制位。同步需要双方都发送自己的初始序号，并且发送确认的 ACK。如图 2-4-8 所示，此交互过程就是所谓的三次握手。

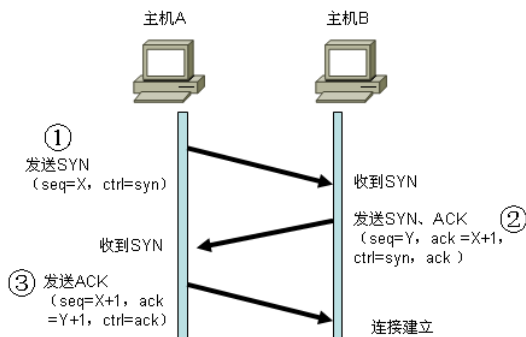


图 2-4-8 TCP 三次握手

- ① 主机 A 发往主机 B，主机 A 的初始序号是 X，设置 SYN 位，未设置 ACK 位。
- ② 主机 B 发往主机 A，主机 B 的初始序号是 Y，确认号 (ACK) 是 X+1，X+1 确认号暗示已经收到主机 A 发往主机 B 的同步序号。设置 SYN 位和 ACK 位。
- ③ 主机 A 发往主机 B，主机 A 的序号是 X+1，确认号是 Y+1，Y+1 确认号暗示已经收到主机 B 发往主机 A 的同步序号。设置 ACK 位，未设置 SYN 位。

三次握手解决的不仅仅有序号问题，还解决了包括窗口大小、MTU（Maximum Transmission Unit，最大传输单元），以及所期望的网络延时等其他问题。

4. 滑动窗口

在大多数可靠、面向连接的数据传输中，数据分组必须以与发送时相同的顺序传输到接收端。任何数据分组丢失、损坏、重复或接收时乱序都将导致协议出错。最基本的解决方法就是让接收方在接收到每一个数据分段后都确认。

如图 2-4-9 所示，如果发送方在发送每一个数据分段后都要等候确认，吞吐量是很低的，因此大多数面向连接、可靠的协议都允许一次发送多个数据分段。因为发送方在发送完数据分组之后和处理完接收到的确认之前是有一段时间间隔的，这段间隔可以用来传输更多的数据。在没有收到确认的情况下，窗口是允许发送方发送数据分组的个数的。

TCP 使用期待确认，即确认号就是所期待接收的下一个字节。滑动窗口是指在 TCP 会话中窗口大小是动态协商的。滑动窗口是一种流控机制，允许源设备在向目的设备发送一定数量的数据之后接收一个确认。

假设窗口大小为 3，如图 2-4-10 所示。源设备可以发送 3 个字节到目的设备，然后需要等待一个确认。目的设备接收到这 3 个字节之后，向源设备返回一个确认，这时候源设备就可以继续传输下面 3 个字节了。如果目的设备没有收到这 3 个字节，它就不会返回确认，源设备没有接收到确认，它就知道这些字节需要重传。

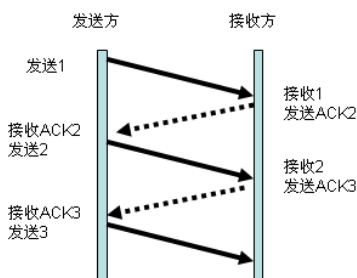


图 2-4-9 窗口大小为 1

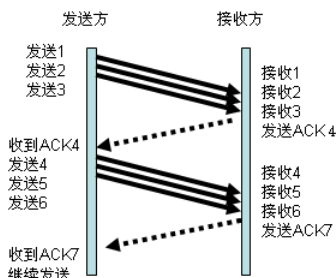


图 2-4-10 窗口大小为 3

5. 确认机制

TCP 在传输前，需要对每个数据分段进行编号。接收端主机将数据分段重组为完整信息，TCP 必须恢复由 Internet 通信系统导致的数据损坏、丢失、重复或乱序。TCP 通过为传输的每个字节指定序号，并且要求接收端 TCP 的主动确认（ACK）来实现，如图 2-4-11 所示。

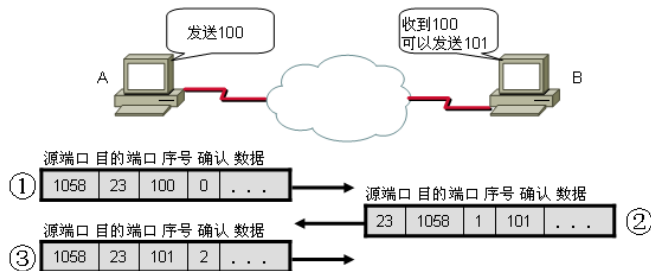


图 2-4-11 TCP 确认机制

① 源主机 A 远程登录目的主机 B，源主机使用一个本地的随机端口 1058，访问目的主机的 23 号服务端口。源主机初始序号是 100，没有确认号。

② 主机 B 收到主机 A 的数据包进行响应，返回的数据包源端口是 23，目的端口是 1058，主机 B 返回的包中的端口号和主机 A 发过来的端口号中的源和目的端口刚好相反。主机 B 的初始序号是 1，确认号 101 表示已经收到主机 A 的序号 100，希望接收序号 101 的包。

③ 主机 A 对主机 B 发过来的包进行响应，发送的序号是 101，确认号 2 表示已经收到主机 B 的序号 1。

2.4.4 应用层***

应用层包括所有的高层协议，与 OSI 的应用层协议相差不大，包括 HTTP（超文本传输协议，使用 TCP 的端口 80）、Telnet（远程登录协议，使用 TCP 的端口 23）、FTP（文件传输协议，使用 TCP 的端口 21 和一个不确定的数据传输端口）、SMTP（简单邮件传输协议，使用 TCP 的端口 25）、POP3（邮局 3 协议，使用 TCP 的端口 110）、DNS（域名服务，使用 UDP 和 TCP 的端口 53）等。



2.5 IP 地址***

IP 地址部分在 CCNA 考试中占了相当大一部分比重。本节主要介绍二进制和十进制的转换、IP 地址的分类、IP 子网划分、子网掩码、公有地址和私有地址等。

IP 地址是用来标识网络中一个通信实体的，比如一台主机，或者是路由器的某一个端口。而在基于 IP 协议网络中传输的数据包，也都必须使用 IP 地址来进行标识，如同我们写一封信，要标明收信人的通信地址和发信人的地址，邮政工作人员通过该地址来决定邮件的去向。

在计算机网络里，每个被传输的数据包也要包括一个源 IP 地址和一个目的 IP 地址。当该数据包在网络中进行传输时，这两个地址要保持不变（有网络地址转换和代理的情况例外，本书后面会介绍到网络地址转换技术），以确保网络设备总能根据确定的 IP 地址，将数据包从源通信实体送往指定的目的通信实体，以及数据包从目的通信实体返回源通信实体。

开始介绍 IP 之前，首先看一上网主机需要配置 TCP/IP 属性中的哪些参数？

打开“Internet 协议（TCP/IP）属性”窗口，如图 2-5-1 所示，一台上网的主机一般需要配置 IP 地址、子网掩码、默认网关、DNS 服务器地址等参数。前面已经介绍了，DNS 服务器用来进行域名解析，负责把域名解析成对应的 IP 地址，可是 IP 地址、子网掩码、默认网关等参数主要起到什么作用呢？本节将对这些参数的用途进行详细说明。

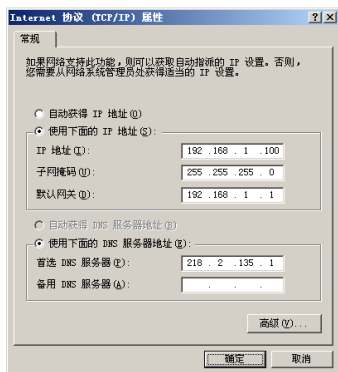


图 2-5-1 “Internet 协议（TCP/IP）属性”配置窗口

2.5.1 二进制和十进制间的转换***

IP 地址使用 32 位二进制数格式，为方便记忆，通常使用以点号分隔的十进制数来表示，如 IP 地址 202.119.248.65 对应的二进制数是 11001010.01110111.11111000.01000001。了解 IP 地址的第一步就是掌握二、十进制间的转换。

1. 二进制转换到十进制

给出一个二进制数 $(1101)_2$ ，该二进制数所对应的十进制是 $1 \times 2^0 + 0 \times 2^1 + 1 \times 2^2 + 1 \times 2^3 = 1 + 0 + 4 + 8 = 13$ 。IP 地址包含 32 个比特，每 8 个比特用 1 个十进制数表示，则每 1 个十进制数最大是 $(11111111)_2 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 128 = 255$ ，从这里可以看出，IP 地址的十进制数表示中，不应该出现超过 255 的数值，从上面的计算中，可以看出在 8 位二进制数的表示中，最高位的 1 表示十进制数的 128，次高位的 1 表示十进制数的 64，再其次是 32……，最低位的 1 表示十进制数的 1。根据这种对应，多数情况下，不需要计算，就可得出二进制数对应的十进制数，譬如 $(10000001) = 128 + 1 = 129$ 。

2. 十进制转换到二进制

很多读者都害怕十进制数到二进制数的转换，因为“除 2 取余”的方法实在是太麻烦了，且容易出错。这里介绍一种简单不易出错的方法，这里姑且称做“凑数字法”，就是把 IP 地址中对应的十进制数凑成 128, 64, 32, 16, 8, 4, 2, 1 等数字的组合，然后从高位到低位，如果出现这个数字就填 1，没有出现的数字填 0，最后得出的 8 位二进制组就是该十进制数对应的二进制数。譬如要把十进制数的 130 和 49 转换成二进制数， $130 = 128 + 2 = (10000010)_2$ ， $49 = 32 + 16 + 1 = (00110001)_2$ 。读者可能会担心，要是出现个大的十进制数怎么转换呀？不要忘了，十进制数表示的 IP 地址，最大不会超过 255。这个方法够简单吧，且不容易出错，读者只要稍加练习，即可熟练掌握。

2.5.2 IP 地址分类***

一个 IP 地址主要由两部分组成：一部分用于标识该地址所从属的网络号；另一部分用于指明该网络上某个特定主机的主机号。网络号由因特网权力机构分配，主机地址由各个网络的管理员统一分配。因此，网络地址的唯一性与网络内主机地址的唯一性确保了 IP 地址的全球唯一性（其中保留给某些网络使用的私有地址段除外）。

为适应不同规模的网络，IP 地址空间被划分为五个不同的地址类别，即 A、B、C、D 和 E 类，如表 2-5-1 所示，其中 A、B、C 三类最为常用，D 类用于组播，E 类用于科研。

表 2-5-1 IP 地址分类表

IP 地址类型	第一字节十进制范围	二进制固定最高位	二进制网络位	二进制主机位	每个网络中可容纳主机数
A	0~127*	0	8 位	24 位	$2^{24}-2$
B	128~191	10	16 位	16 位	$2^{16}-2$
C	192~223	110	24 位	8 位	2^8-2
D	224~239	1110	组播地址使用		
E	240~255	1111	保留实验使用		

*规定 A 类中的 0 不允许使用，127 作为测试 TCP/IP 协议的环回地址，也不可以使用，因此 A 类实际可用的地址是 1~126。

1. A 类地址

A 类地址用来支持超大网络，A 类 IP 地址的前 8 位二进制表示网络号，后 24 位二进制表示主机号。A 类地址很好识别，只需把第一个十进制数换算成二进制数，如果最高位是“0”，则是 A 类地址，但有两个特例，0 和 127 两个数被保留，不属于 A 类地址。A 类地址的范围从 1~126，全球只有 126 个 A 类网络。如果申请到一个 A 类地址就相当于申请到 2^{24} 个 IP 地址，等于 16 777 216 个。

2. B 类地址

B 类地址用来支持中等网络，B 类 IP 地址的前 16 位二进制表示网络号，后 16 位二进制表示主机号。B 类地址很好识别，只需把第一个十进制数换算成二进制数，如果前两位是“10”，则是 B 类地址，范围从 $(10000000)_2=128$ 到 $(10111111)_2=191$ 。全球有 2^{14} 个 B 类网络。如果申请到一个 B 类地址就相当于申请到 2^{16} 个 IP 地址，等于 65 536 个。

3. C 类地址

C 类地址用来支持小型网络，C 类 IP 地址的前 24 位二进制表示网络号，后 8 位二进制表示主机号。C 类地址很好识别，只需把第一个十进制数换算成二进制数，如果前三位是“110”，则是 C 类地址，范围从 $(11000000)_2=192$ 到 $(11011111)_2=223$ 。全球有 2^{21} 个 C 类网络。如果申请到一个 C 类地址就相当于申请到 2^8 个 IP 地址，等于 256 个。

4. D 类地址

D 类地址用来支持组播，也称组播地址。组播地址不区分网络号或主机号，就是单一的网络地址，用来转发目的地址为预先定义的一组 IP 地址的分组。因此，一台工作站可以将单一的数据流同时传送给多个接收者。D 类地址也很好识别，只需把第一个十进制数换算成二进制数，如果前四位是“1110”，则是 D 类地址，范围从 $(11100000)_2=224$ 到 $(11101111)_2=239$ 。全球有 2^{28} 个组播地址。

5. E 类地址

E 类地址用于科研，因此，Internet 上没有 E 类地址。E 类地址也很好识别，只需把第一个十进制数换算成二进制数，如果前四位是“1111”，则是 E 类地址，范围从 $(11110000)_2=240$ 到 $(11111111)_2=255$ 。

2.5.3 保留 IP 地址***

注意表 2-5-1 中每个网络中可容纳的主机数都是申请的 IP 地址减去 2，这是因为有一些地址被保留，不能分配给网络中的设备使用。每个网络中保留的两个 IP 地址是：

- **网络地址：**网络位不变，主机位全 0 的 IP 地址代表网络本身，不能分配给某个网络设备使用。
- **广播地址：**网络位不变，主机位全 1 的 IP 地址代表本网络的广播，也不能分配给某个网络设备使用。发往广播 IP 地址的数据包被本网络中所有主机接收。

譬如，默认 C 类网络 192.168.1.0 中，IP 地址的范围从 192.168.1.0 到 192.168.1.255，排除网络地址 192.168.1.0 和广播地址 192.168.1.255，192.168.1.0 网络中可以使用的 IP 地址数是 254 个。默认 B 类网络 172.16.0.0 中，IP 地址的范围从 172.16.0.0 到 172.16.255.255，排除网络地址 172.16.0.0 和广播地址 172.16.255.255，172.16.0.0 网络中可以使用的 IP 地址数是 $65536-2=65534$ 个，这里特别要提醒的是 172.16.0.255、172.16.1.255……172.16.254.255 并不是广播地址，因为 B 类网络地址的主机位有 16，只有 16 位全是 1 才是广播地址。

本节的后面部分会介绍到 IP 子网划分，请牢牢记住一点，即：主机位全 0 的是网络地址，主机位全 1 的是广播地址。

2.5.4 公有 IP 地址和私有 IP 地址**

公有 IP 地址是唯一的，因为公有 IP 地址是全局的和标准的，所以没有任何两台连到公

共网络的主机拥有相同的 IP 地址。一般宽带接入用户可以花些费用，向 ISP 运营商申请公有的 IP 地址，拥有公有 IP 地址后，就可以向因特网提供服务了。

随着 Internet 的快速增长，公有 IP 地址几近枯竭。为解决这个问题，提出了 VLSM（Variable Length Subnet Masks，变长子网掩码）、CIDR（Classless Inter-Domain Routing，无类别域间路由），以及 IPv6 等机制。有关 VLSM、CIDR 和 IPv6 将在本书后面的章节中讨论。

另一种更行之有效的方法是使用私有地址。如前所述，Internet 主机需要一个全局唯一的 IP 地址。可是私有网络不连接到 Internet 上，它可以使用任何有效的 IP 地址。如果私有网络需要连接到 Internet 上，可以使用代理或具有 NAT（Network Address Translation，网络地址转换）能力的设备进行转换，把私有 IP 地址转换成合法的公有 IP 地址，再访问 Internet。

原则上讲，私有网络可以配置任何有效的 IP 地址，可有一个问题出现了，如果私网中配置的是 202.119.248.0 这个 C 类网络，该私有网络将无法访问南京工业大学的 Web 主页，因为南京工业大学 Web 服务器的 IP 地址是 202.119.248.65，私有网络的主机将会在局域网中寻找 202.119.248.65，而不会把数据包发往正确的 Internet。为了避免出现这种情况，RFC1918 留出 3 块专有的 IP 地址空间（1 个 A 类地址段，16 个 B 类地址段，256 个 C 类地址段，如表 2-5-2 所示）作为私有的内部使用的地址。在这 3 块范围内的 IP 地址不会被 Internet 的路由器转发，因为 Internet 上的路由器均没有配置这些 IP 地址的路由，如果有去往这些私有 IP 地址的数据包将被路由器丢弃。

表 2-5-2 私有 IP 地址

IP 地址类别	RFC1918 规定的地址范围
A	10.0.0.0~10.255.255.255
B	172.16.0.0~172.31.255.255
C	192.168.0.0~192.168.255.255

2.5.5 IP 子网划分***

在讲述子网划分之前，先来看一个实例，如图 2-5-2 所示，4 台计算机接在一个 HUB（集线器）上，IP 和子网掩码配置如图中所示。图中的“/24”表示计算机 IP 地址的网络位有 24 位，主机位是 8 位（ $32-24=8$ ，相当于子网掩码是 255.255.255.0，CCNA 考题中经常用这种格式表示子网掩码）。图中哪些计算机之间可以通信？判断的依据是什么？如何才能让它们全部都可以互访？

答案是 PC1（Personal Computer，个人计算机）和 PC3 为一组，PC2 和 PC4 为一组，组内计算机之间可以通信，组间计算机之间不能通信。判断的依据是：同一子网的计算机可以直接通信，不同子网的计算机不可以直接通信。处在不同子网中的计算机间如需通信，需要通过一个三层设备，也就是有路由功能的设备。前面已经介绍过集线器处在物理层，不具有网络层的功能，不能实现不同网络间的互连。

那么如何判断在不在同一个子网呢？先把 IP 地址和子网掩码转换成二进制数，然后进行“与”运算，也就是二进制数的按位取小运算，得出一台计算机所在的网络号，如果两

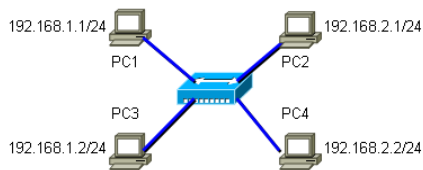


图 2-5-2 计算机互访图

台计算机的网络号相同，就说明它们处在同一子网；如果网络号不同，就说明它们处在不同子网。把每台计算机的 IP 地址与子网掩码进行按位“与”运算，我们得出 PC1 的网络号是 192.168.1.0/24，PC2 的网络号是 192.168.2.0/24，PC3 的网络号是 192.168.1.0/24，PC4 的网络号是 192.168.2.0/24，PC1 和 PC3 处在同一子网，PC2 和 PC4 处在同一子网。如果 192.168.1.0 网络中的计算机需要访问 192.168.2.0 网络中的计算机，那么就需要通过一个三层设备，而 HUB 处于 OSI 七层模型中的第一层，即物理层，不具备路由功能，无法为不同子网中的计算机提供路由功能。

如何才能让 4 台计算机相互之间都可以通信呢？方法有很多种，这里简单列举 3 种。

- **方法一：**修改 PC2、PC4 的 IP 地址为 192.168.1.3、192.168.1.4，这样 4 台计算机就处在同一子网中，相互之间可以直接通信。这种方法有一定的局限性，假如 192.168.1.0/24 网中已经有 254 台计算机，如果又有新的计算机加入，192.168.1.0/24 网段中所有有效的 IP 地址都被分配出去，新加入的计算机将无 IP 地址可用，此时就需使用方法二了。
- **方法二：**修改 4 台计算机的子掩码为“/22”，即 255.255.252.0，这样 4 台计算机的网络号都是 192.168.0.0/22，处在同一个子网中，这样的子网中，网络位有 22 位，主机位有 10 位，可以容纳的主机数为 $2^{10}-2=1022$ 台，即从 192.168.0.1 到 192.168.3.254。这种方法也有不足之处，因处在同一个子网中的计算机处在同一个广播域，一是存在安全隐患；二是大量广播存在，影响通信效率；三是故障排除困难，如果同一个子网中的计算机数量过多，可以考虑采用第三种方法。
- **方法三：**把集线器换成三层交换机，并把接 PC1、PC3 的交换机端口划到一个 VLAN（Virtual Local Area Network，虚拟局域网，在本书后面章节会更详细深入地讨论 VLAN 的配置），并给此 VLAN 分配 IP 地址 192.168.1.254，把 PC1 和 PC3 的网关设成 192.168.1.254。把接 PC2、PC4 的交换机端口划到另一个不同的 VLAN，并给此 VLAN 分配 IP 地址 192.168.2.254，把 PC2 和 PC4 的网关设成 192.168.2.254。这样 4 台计算机之间也可相互通信了。三层交换机可以把两个子网连通起来，三层交换机有两个 VLAN，每个 VLAN 都是一个广播域，两个 VLAN 中的广播互不影响。第三种方法可以有效地克服第二种方法的不足，缺点就是增加了硬件设备的投资。

在做子网划分的时候有一点需要注意，主机位全“0”、全“1”的 IP 地址都不可以使用，全“0”的是子网地址，全“1”的是子网广播地址，如 192.168.1.0/24 和 192.168.1.255/24 这两个 IP 地址就分别代表网络地址和广播地址，都不可以配置给计算机使用。192.168.0.0/22 和 192.168.3.255/22 这两个 IP 地址也分别代表了网络地址和广播地址，也不可以配置给计算机使用，而 192.168.1.0/22、192.168.2.0/22、192.168.3.0/22、192.168.0.255/22、192.168.1.255/22、192.168.2.255/22 则可以分配给计算机使用。192.168.1.0/24 网络中可用的 IP 地址数是 $256-2=254$ 个，192.168.0.0/22 网络中可用的 IP 地址数是 $1024-2=1022$ 个，即每个子网中可用的 IP 地址数量是： $2^{\text{主机位数}}-2$ 。

1. 为何要划分子网


在讲述子网划分之前，先来分析一下为何要划分子网？因为划分子网主要有下列好处：

- 缩减网络流量，优化网络性能。在前面介绍的方法三中，大家知道在不同子网中的广播地址互不相同，而在相同子网中的广播地址是相同的。试想一下，如果申请到一个 B 类的地址 173.1.0.0/16，该子网中可以容纳的主机数是 65534 台，6 万多台的

计算机在同一个子网中，广播量非常巨大。通过三层交换机或路由器把 6 万多台计算机隔离到不同的子网中，大多数的流量将会被限制在本地子网中，而只有那些被标明发送到其他网络的流量，才会通过路由器或三层交换机的网络层。路由器和三层交换机的 VLAN 创建了广播域，创建的广播域越多，其广播域的规模就越小，并且在每个网段上的无关流量也就会越低。

- 简化管理。与一个巨大的网络相比，在一组较小的互联网络中，判断并孤立网络所出现的故障会容易很多。
- 增加网络安全性。试想一下，如果申请到一个 C 类的地址 193.1.1.0/24，公司内部多个部门共同使用这个 C 类地址，相互之间处在同一个广播域，通过使用黑客工具，可以很容易地截获其他用户之间的通信，存在很大的安全隐患，且不容易实现访问控制。通过划分子网，让路由器互连不同的子网，在路由器上配置 ACL (Access Control List，访问控制列表) 限制不同网络之间的访问权限，提高网络的安全性。

2. 如何创建子网

 **例 1:** 假如某单位申请到了一个 C 类的网络地址 199.1.1.0/24，该单位共有 5 个部门，每个部门最多只会有 28 台计算机。为了增强安全性，使用路由器来限制部门之间只能进行有限的访问。问子网掩码设成多少比较合适？每个部门使用的 IP 地址范围是多少？

分析 C 类地址的特征，24 位网络位，8 位主机位，因为网络位是由 IP 地址分配商提供，固定不变的，单位内部可以调整的只能是主机位。如果从 8 位主机位中借出一位来延长网络位，只能划分成 $2^1=2$ 个子网（有些老式系统不支持全“0”和全“1”的子网，也就是子网位是全“0”和全“1”的网络号。在这种情况下，如果是借 1 位，将没有子网可用，但新的系统基本都不存在这个限制，思科路由器上可以在全局配置模式下使用“Router(config)#ip subnet-zero”命令让路由器支持全“0”和全“1”的子网，使用“Router(config)#no ip subnet-zero”命令让路由器不支持全“0”和全“1”的子网。在 CCNA 考试中，在没有特别说明是否支持全“0”和全“1”子网的情况下，默认是不支持的，有关这一点，考生要特别注意），满足不了 5 个部门的需要；借 2 位，可以划分成 $2^2=4$ 个子网，还是满足不了 5 个部门的需要；借 3 位，可以分成 $2^3=8$ 个子网，可以满足 5 个部门使用的需要。网络位本来有 24 位，又从主机位借走了 3 位作为子网位，还剩下 5 位主机位，每个子网可容纳的主机数量是 $2^5-2=30$ ，大于每个部门最多的主机数量 28；借 4 位，虽然子网数量满足了，可主机位只剩下 4 位，每个子网中最多只能有 $2^4-2=14$ 个可用 IP 地址，还要去除网关占用的一个 IP 地址，每个子网最多只能容纳 13 台计算机，小于每个部门最多有 28 台计算机的需求。故本例的正确划分方法只有一种，从主机位中借出 3 位作为子网位，则网络位变成了 $24+3=27$ 位，换成十进制就是 255.255.255.224。

本例中，通过从一个 C 类地址的主机位中借出 3 位，分成了如下 8 个子网：

000
001
010
011
100
101
110

111

即:

199.1.1.0/27

199.1.1.32/27

199.1.1.64/27

199.1.1.96/27

199.1.1.128/27

199.1.1.160/27

199.1.1.192/27

199.1.1.224/27

而单位只需有 5 个子网, 默认不使用全“0”和全“1”的子网, 即不使用 199.1.1.0/27 和 199.1.1.224/27 的子网, 从剩下的 6 个子网中拿出前 5 个子网, 最后的 1 个子网预留给将来的升级使用, 如果单位增加了新的部门将可以使用该子网。第一个可用子网 199.1.1.32/27 的 IP 地址范围从 $199.1.1.(00100000)_2$ 到 $199.1.1.(00111111)_2$, 即从 199.1.1.32 到 199.1.1.63, 共包括 32 个 IP 地址。其中 199.1.1.32/27 的主机位全“0”, 是网络地址, 也是本子网中第一个 IP 地址, 不可以使用。199.1.1.63/27 的主机位全“1”, 是该子网的广播地址, 也是本子网中最后一个 IP 地址, 不可以使用。假设每个子网都是把第一个可以使用的 IP 地址用做网关, 则 199.1.1.33 配在路由器的接口上, 充当本子网的默认网关。则本子网中主机可以使用的 IP 地址是从 199.1.1.34 到 199.1.1.62, 共 29 个。所有子网的 IP 地址范围、网络号、子网广播、网关、主机可用 IP 地址范围、网络掩码等, 如表 2-5-3 所示。

表 2-5-3 IP 地址划分

子网位	IP 范围	网络号	子网广播	网关	主机可用 IP	掩码
000: 全“0”子网默认不可以使用						
001	32~63	199.1.1.32	199.1.1.63	199.1.1.33	34~62	/27
010	64~95	199.1.1.64	199.1.1.95	199.1.1.65	66~94	/27
011	96~127	199.1.1.96	199.1.1.127	199.1.1.97	98~126	/27
100	128~159	199.1.1.128	199.1.1.159	199.1.1.129	130~158	/27
101	160~191	199.1.1.160	199.1.1.191	199.1.1.161	162~190	/27
110 (暂未使用)	192~223	199.1.1.192	199.1.1.223	199.1.1.193	194~222	/27
111: 全“1”子网默认不可以使用						

本例中, 计算机的 IP 地址、子网使用、路由器接口的配置等, 如图 2-5-3 所示。

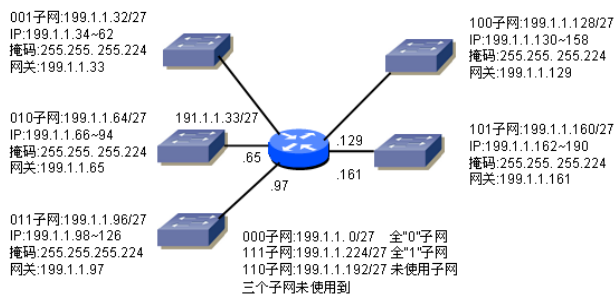


图 2-5-3 子网的划分

例 2：一台计算机的 IP 地址和子网掩码是 172.16.2.160/26，如何计算出该计算机所在的子网地址、子网广播地址、该子网中第一个可用的 IP 地址、该子网中最后一个可用的 IP 地址、该子网中共有多少个 IP 地址可用？

如何对上述问题进行解答，许多行家一眼就能看出答案，但对于初学者却非易事，这里介绍几种解法，读者可以根据习惯任选一种。

解法一：图 2-5-4 给出了一个通用的解法，虽然有点烦琐，但却易于理解，不会出错，随着对“与”运算的了解，还是可以再做精简的。下面对图中的 9 个步骤解释如下：

步骤 1：把 IP 地址换成二进制数，不要使用一般常用的“除 2 取余”法，特别容易搞错。建议使用前面介绍过的“凑数字法”。最后会发现，本例中的 172.16.2 是没有必要换成二进制数的，因为它们是与 255.255.255 进行与运算，任何数与 255 与运算的结果一定是它本身。

步骤 2：把子网掩码换成二进制数。

步骤 3：在子网掩码二进制数表示法中“1”的结束处，画一条竖线，竖线左边表示的是网络位，竖线右边表示的是主机位。本例中网络位是 26 位，主机位是 6 位。授课中，有的学生可能会问，如果“1”的位数不连续怎么办，事实上网络位在前，主机位在后，网络位是连续的，不会出现网络位与主机位交叉的情况。

步骤 4：主机位全是“0”的地址是子网地址。

步骤 5：主机位全是“1”的地址是广播地址。

步骤 6：子网地址加 1 得到的是本子网中第一个可用的 IP 地址。

步骤 7：子网广播地址减 1 得到的是本子网中最后一个可用的 IP 地址。

步骤 8：把 IP 地址在竖线左边的网络位部分照抄下来，把各个地址部分补充完整。

步骤 9：把二进制数转换成十进制数，就得出了本子网地址是 172.16.2.128，本子网广播地址是 172.16.2.191，本子网中第一个可用的 IP 地址是 172.16.2.129，本子网中最后一个可用的 IP 地址是 172.16.2.190，本子网可用的 IP 地址数量是 $2^6-2=62$ 个。

解法二：考虑到计算机 172.16.2.160/26 所处的子网是一个比 C 类地址还小的地址空间，可以想象成是一个 C 类地址被子网划分。每个子网中的 IP 地址数是 $2^6=64$ ，被分成的 4 个子网的 IP 地址范围是：

172.16.2.0~63

172.16.2.64~127

172.16.2.128~191

172.16.2.192~255

172.16.2.160 落在第三个子网范围 172.16.2.128~191 中，该子网中第一个 IP 地址是网络号，即 172.16.2.128；该子网中最后一个 IP 地址是子网广播地址，即 172.16.2.191；该子网中第一个可用的 IP 地址是子网地址加 1，即 172.16.2.129；该子网中最后一个可用的 IP 地址是广播地址减 1，即 172.16.2.190；该子网中可用的 IP 地址数是 $2^6-2=62$ 个，即 IP 地址范围中排除子网地址和广播地址。

例 3：在图 2-5-5 中，路由器 R1、R2、R4 上均有 4 个 C 类的地址，路由器 R3 能学

	172	16	2	160	
					3
172.16.2.160	10101100	00010000	00000010	10100000	Host 1
255.255.255.192	11111111	11111111	11111111	10000000	Mask 2
172.16.2.128	10101100	00010000	00000010	10000000	Subnet 4
172.16.2.191	10101100	00010000	00000010	10111111	Broadcast 5
172.16.2.129	10101100	00010000	00000010	10000001	First 6
172.16.2.190	10101100	00010000	00000010	10111110	Last 7

图 2-5-4 子网的计算

到所有的路由条目（有关路由，本书后面有专门的章节介绍，这里关心的只是 IP 地址计算问题）。R3 的路由表中有 $12+3$ （路由器间的互连网段）=15 个条目，过多的路由表条目会占用更多的内存，耗用更多的 CPU，还会带来网络的不稳定性。可以使用路由汇总技术来减小 R3 路由表的大小。

把所有明细路由条目转换成二进制形式，把共同的部分取出来，即可实现路由的汇总。这里以 R1 上的 4 个条目为例，按图 2-5-6 所示进行操作：

步骤 1：①②③④ 4 个步骤把 4 个明细路由条目转换成二进制形式。

步骤 2：⑤ 在所有明细条目共同部分的后面画一条竖线。

步骤 3：⑥ 取出共同的部分，后面的位补“0”，这里是 191.1.0.0。再数一数竖线左边的位数是 22，得出汇总后的网络地址是 191.1.0.0/22。同理可以得出去往 R2 的路由汇总条目是 191.1.4.0/22，去往 R4 的路由汇总条目是 191.1.8.0/22。

步骤 4：在 R3 上取消明细条目，只保留汇总后的条目（学完路由部分，读者就可以动手配置了）。路由表条目从汇总前的 15 条变成汇总后的 3（汇总后的路由）+3（路由器中的互连网段）=6 条，路由表大大减小。

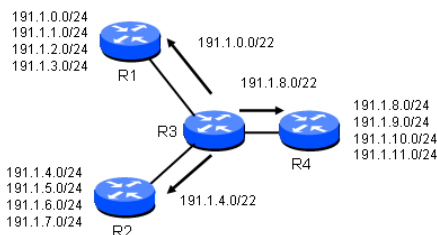


图 2-5-5 路由汇聚

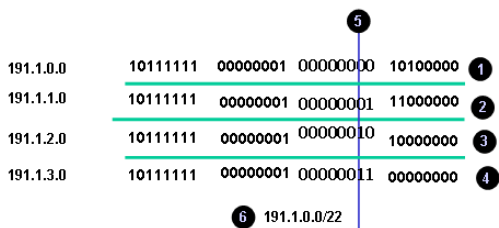


图 2-5-6 路由汇总算法

IP 地址的计算在 CCNA 考试中占有相当大的比重，所以仅了解这几个例子还远远不够，需完成章节后面的真题，并仔细阅读解题方法和思路。此外，本书第 6.3 节介绍的 VLSM 也属于 IP 地址的计算问题。



2.6 封装和解封装***

数据的封装和解封装在 CCNA 考试中，几乎每次必考。明白数据的封装和解封装对大家理解数据包在网络中的传输也相当重要，本节结合一个实例，讲解数据包在网络中的流动。其实数据包在网络中的流动就是一个重复的封装和解封装的过程。本节的讲解请参考光盘中的视频文件“视频2-2.wrf”。

在图 2-6-1 中，PC1 远程登录（Telnet）服务器，整个过程是如何实现的呢？下面列出具体的实现步骤。

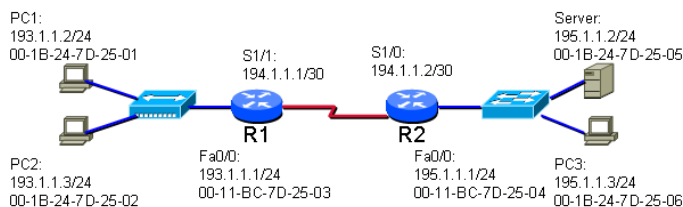


图 2-6-1 数据包在网络中的流动

步骤1: PC1 封装数据包。PC1 比较要去往的目标 IP 地址,发现服务器的 IP 地址 195.1.1.2 不在本地网络中,PC1 知道要发往不同网络中的数据包,首先要发往网关,也就是图中路由器 R1 快速以太网接口 Fa0/0 的 IP 地址 193.1.1.1。PC1 查询本地的 ARP 缓存,如果找到 193.1.1.1 对应的 MAC 地址则进行封装;如果在 ARP 缓存中没有找到 193.1.1.1 对应的 MAC 地址,则用前面章节介绍过的 ARP 协议,查询到网关对应的 MAC 地址“00-11-BC-7D-25-03”。

PC1 对 Telnet 协议的数据包进行封装,首先在传输层进行分段等处理。因 Telnet 使用的是 TCP 协议,PC1 使用本地一个大于 1024 以上的随机 TCP 源端口(这里假设是 1030)建立到目的服务器 TCP 23 号端口的连接,TCP 源端口和目的端口被加入到传输层的协议数据单元中(Protocol Data Unit, PDU)。如图 2-6-2 所示,协议数据单元在应用层、表示层和会话层被称做数据(Data),在传输层被称做分段(Segment),在网络层被称做包(Packet),在数据链路层被称做帧(Frame),在物理层被称做比特(Bit)。因 TCP 是一个可靠的传输控制协议,传输层还会加入序列号、窗口大小等参数。

传输层封装后的数据分段被传到网络层,封装网络层的头部,主要就是添加源和目的 IP 地址,这里的源 IP 地址是 193.1.1.2,目的 IP 地址是 195.1.1.2。

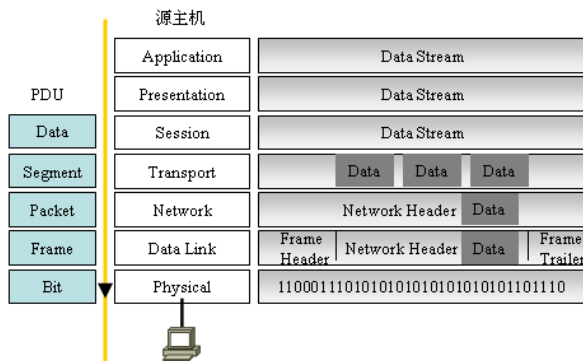


图 2-6-2 数据包封装

网络层封装后的数据包被传到数据链路层,封装帧头和帧尾。帧尾是添加被称做 CRC 的循环冗余校验部分。帧头主要是添加数据链路层的地址,即数据链路层的源地址和目的地址,用在以太网上的体现就是添加源 MAC 地址和目的 MAC 地址,这里的源 MAC 地址是 PC1 的 MAC 地址“00-1B-24-7D-25-01”,目的 MAC 地址是网关的 MAC 地址“00-11-BC-7D-25-03”。有关目的 MAC 地址为何是路由器接口的 MAC 地址,而不是目的服务器网卡的 MAC 地址,是很多读者困惑的地方,当然也是 CCNA 考试的一个考点。我们说 MAC 只是用在局域网内的寻址,如果封装的是目的服务器的 MAC 地址,如何体现这个包是发往路由器的呢?假设封装的目的 MAC 地址是服务器的 MAC 地址“00-1B-24-7D-25-05”,这样的数据包被传到路由器后,路由器比较数据帧中的目的 MAC 地址,发现与本路由器接口的 MAC 地址不同,路由器丢弃这个包,数据包不被路由器转发,更别想能到达目的服务器了。PC1 发出的数据帧格式如图 2-6-3 所示。

帧头部		网络层头部		传输层头部		数据	帧尾
目的	源	目的IP	源IP	目的端口	源端口		
00-11-BC-7D-25-03	00-1B-24-7D-25-01	195.1.1.2	193.1.1.2	23	1030	Telnet 数据	CRC 检验

图 2-6-3 PC1 发出的数据帧格式

数据链路层封装后的数据帧被传到物理层，转换成二进制形式的比特（Bit）流，从 PC1 的网卡发送出去。物理层的用途就是处理比特流，把比特转换成电子、光学或微波信号。反之在接收端，物理层从传输媒体中重新得到这些信号，恢复成比特流，传输比特流到数据链路层。

步骤 2：PC1 发出的比特流到达集线器（注意图 2-6-1 中的图标表示的是集线器），集线器简单地对比特流进行放大，从除接收端口以外的所有端口转发出去。PC2 接收到这个数据包，把比特流转换成帧上传到数据链路层，PC2 比较数据帧的目的 MAC 地址，发现与本机网卡的 MAC 地址不同，PC2 丢弃该数据帧，放弃处理。

步骤 3：路由器 R1 收到该比特流，转换成帧上传到数据链路层，路由器 R1 比较数据帧的目的 MAC 地址，发现与路由器接收端口 Fa0/0（FastEthernet，快速以太网，简写成 Fa0/0，指的是 0 号插槽上编号为 0 的接口）的 MAC 地址相同，路由器知道该数据帧是发往本路由器的。路由器 R1 的数据链路层把数据帧进行解封，然后上传到路由器 R1 的网络层，路由器 R1 看到数据包的目的 IP 地址是 195.1.1.2，并不是发给本路由器的，需要路由器进行转发。

路由器 R1 查询自己的路由表，发现数据包应该从串行接口 S1/1 发出。路由器 R1 把数据包从 Fa0/0 接口交换到 S1/1 接口。

此时 R1 并不能直接把这个数据包发出去，因为在 R1 的 Fa0/0 接口被解封，现在需要被重新再封装。可以想象一个风雪交加的日子，进门的时候拿下帽子，出门的时候需要再戴上帽子。数据封装也是这样，在路由器的入接口解封，在路由器的出接口需要再封装，和人取下帽子有区别的是，这里解封去掉的内容和再封装加上内容是不一样的。网络层的封装并没有被解开，但并不意味着网络层的信息一点都没有改变，其实网络层的数据包中源和目的 IP 地址都没有被改变（除非在网络地址转换的情况下），但 TTL（生存周期，前面已经介绍过）会减 1。网络层把数据包交给下层的数据链路层，数据链路层需要封装二层的地址。串行链路不同于以太网，因为以太网是一个多路访问的网络，要定位到目的设备需要借助于 MAC 地址，但串行线路一般的封装协议都是 PPP（Point-to-Point Protocol，点到点协议）或 HDLC（High-Level Data Link Control，高级数据链路控制协议）封装，这种封装被用于点对点线路，也就是说，一根线缆只连接两台设备，一端发出，另一端肯定可以收到。假设串行线缆上使用的是 PPP 协议，则数据链路层封装的源和目的地址都是 PPP。路由器 R1 发出的数据帧格式如图 2-6-4 所示。

数据链路层封装后的数据帧被传到物理层，转换成二进制形式的比特流，从路由器 R1 的 S1/1 接口发送出去。

帧头部		网络层头部		传输层头部		数据	帧尾
目的	源	目的 IP	源 IP	目的端口	源端口		
PPP	PPP	195.1.1.2	193.1.1.2	23	1030	Telnet 数据	CRC 检验

图 2-6-4 路由器 R1 发出的数据帧格式

步骤 4：路由器 R2 收到这个比特流，上传至数据链路层，数据链路层去掉 PPP 的封装。路由器 R2 查询数据包的目的 IP 地址，发现该 IP 网络直接连接在 Fa0/0 接口，路由器 R2 把数据包交换到 Fa0/0 接口。路由器查看本地的 ARP 缓存，如果找到 195.1.1.2 对应的 MAC 地址，则直接进行封装；如果没有找到，则发送 ARP 的查询包。路由器 R2 发出数据帧的

源地址是 Fa0/0 接口的 MAC 地址，目的地址是服务器网卡的 MAC 地址。路由器 R2 发出的数据帧格式如图 2-6-5 所示。

帧头部		网络层头部		传输层头部		数据	帧尾
目的	源	目的IP	源IP	目的端口	源端口		
00-1B-24-7D-25-05	00-11-BC-7D-25-04	195.1.1.2	193.1.1.2	23	1030	Telnet数据	CRC检验

图 2-6-5 路由器 R2 发出的数据帧格式

数据链路层封装后的数据帧被传到物理层，转换成二进制形式的比特流，从路由器 R2 的 Fa0/0 接口发送出去。

步骤 5: 路由器 R2 发出的比特流到达交换机（注意图 2-6-1 中的图标表示的是交换机），交换机除了对比特流进行放大外，还根据源 MAC 地址进行学习，根据目的 MAC 地址进行转发。交换机根据数据帧中的目的 MAC 地址查询 MAC 地址表，把比特流从对应的端口发送出去，交换机把比特流发往服务器，并没有发往 PC3。

步骤 6: 服务器接收到这个比特流，把比特流转换成帧格式，上传到数据链路层，服务器发现数据帧中的目的 MAC 地址与本网卡的 MAC 地址相同，服务器拆除数据链路层的封装后，把数据包上传到网络层。服务器的网络层比较数据包中的目的 IP 地址，发现与本机的 IP 地址相同，服务器拆除网络层的封装后，把数据分段上传到传输层。传输层对数据分段进行确认、排序、重组，确保数据传输的可靠性。

数据最后被传到服务器的应用层。从 PC1 到 Server 的整个数据包流动过程如图 2-6-6 所示，从图中可以看出，PC1 执行 OSI 七层的封装，然后把比特流传到集线器；集线器在物理层把信号简单放大后，把比特流传到路由器 R1；R1 执行 OSI 下三层的处理后，再把比特流传到路由器 R2；R2 执行 OSI 下三层的处理后，再把比特流传到交换机；交换机执行 OSI 下二层的处理后，再把比特流传到服务器。

从这个流动过程中，可以发现数据流在中间设备上主要执行的是 OSI 下三层的操作，物理层的设备不改变帧的格式，广播式转发；数据链路层的设备也不改变帧的格式，但可以根据数据帧中的目的 MAC 地址进行转发；网络层的设备改变帧的格式，要执行帧的解封封装和再封装，但不改变数据包中的源和目的 IP 地址。

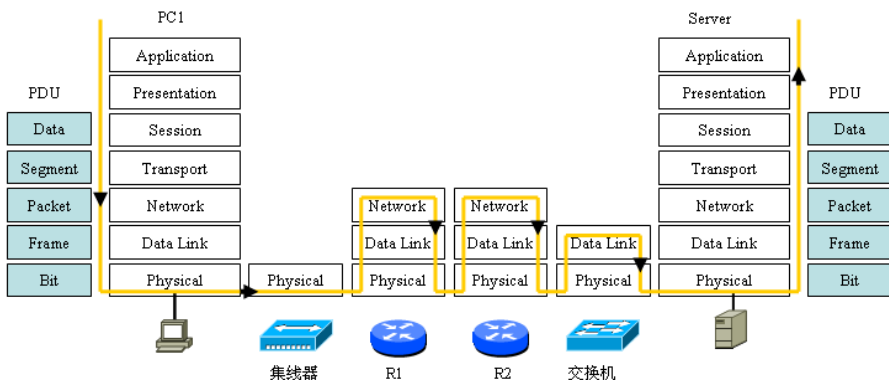


图 2-6-6 封装和解封装

步骤 7: 服务器收到 PC1 发过来的 Telnet 包后，对 PC1 进行响应。和 PC1 处理的过程类似，服务器也知道要发往一个远程的网络，数据链路层的目的 MAC 地址需要封装网关的

MAC 地址；网络层源和目的 IP 地址与 PC1 发送过来的包相反，即把源地址变成目的地址，目的地址变成源地址；传输层源和目的端口与 PC1 发送过来的包相反，即把源端口变成目的端口，目的端口变成源端口。服务器发回的数据帧格式如图 2-6-7 所示。

帧头部		网络层头部		传输层头部		数据	帧尾
目的	源	目的IP	源IP	目的端口	源端口		
00-11-BE-7D-25-04	00-1B-24-7D-25-05	193.1.1.2	195.1.1.2	1030	23	返回数据	CRC 检验

图 2-6-7 服务器发回的数据帧格式



2.7 真题精选***

1. Which two topologies are using the correct type of twisted-pair cables? (Choose two.)

☐ A.

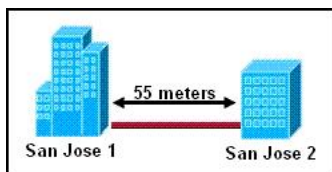
☐ B.

☐ C.

☐ D.

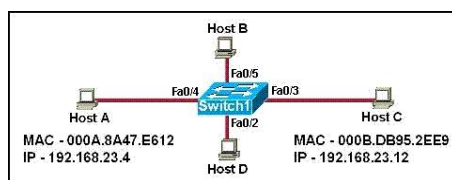
☐ E.

2. Refer to the exhibit. Two buildings on the San Jose campus of a small company must be connected to use Ethernet with a bandwidth of at least 100 Mbps. The company is concerned about possible problems from voltage potential differences between the two buildings. Which media type should be used for the connection?



A. UTP cable B. STP cable C. coaxial cable D. fiber optic cable

3. Refer to the exhibit. Switch1 has just been restarted and has passed the POST routine. Host A sends its initial frame to Host C. What is the first thing the switch will do as regards populating the switching table?



- A. Switch1 will add 192.168.23.4 to the switching table.
- B. Switch1 will add 192.168.23.12 to the switching table.
- C. Switch1 will add 000A.8A47.E612 to the switching table.
- D. Switch1 will add 000B.DB95.2EE9 to the switching table.

4. Refer to the exhibit. Switch-1 needs to send data to a host with a MAC address of 00b0.d056.efa4. What will Switch-1 do with this data?

Switch-1# show mac address-table			
Dynamic Addresses Count:			3
Secure Addresses (User-defined) Count:			0
Static Addresses (User-defined) Count:			0
System Self Addresses Count:			41
Total Mac addresses:			50
Non-static Address Table:			
Destination Address	Address Type	VLAN	Destination Port
0010.0de0.e289	Dynamic	1	FastEthernet0/1
0010.7b00.1540	Dynamic	2	FastEthernet0/3
0010.7b00.1545	Dynamic	2	FastEthernet0/2

- A. Switch-1 will drop the data because it does not have an entry for that MAC address.
- B. Switch-1 will flood the data out all of its ports except the port from which the data originated.
- C. Switch-1 will send an ARP request out all its ports except the port from which the data originated.
- D. Switch-1 will forward the data to its default gateway.
- 5. Why will a switch never learn a broadcast address?
 - A. Broadcasts only use network layer addressing.
 - B. A broadcast frame is never forwarded by a switch.
 - C. A broadcast address will never be the source address of a frame.
 - D. Broadcast addresses use an incorrect format for the switching table.
 - E. Broadcast frames are never sent to switches.
- 6. What will an Ethernet switch do if it receives a unicast frame with a destination MAC that is listed in the switch table?
 - A. The switch will not forward unicast frames.
 - B. The switch will forward the frame to a specific port.
 - C. The switch will return a copy of the frame out the source port.
 - D. The switch will remove the destination MAC from the switch table.
 - E. The switch will forward the frame to all ports except the port on which it was received.
- 7. Which of the following is true regarding the use of switches and hubs for network connectivity?
 - A. Switches take less time to process frames than hubs take.

- B. Switches do not forward broadcasts.
 - C. Hubs can filter frames.
 - D. Using hubs can increase the amount of bandwidth available to hosts.
 - E. Switches increase the number of collision domains in the network.
8. Which of the following statements are true regarding bridges and switches?

(Choose 3.)

- A. Switches are primarily software based while bridges are hardware based.
 - B. Both bridges and switches forward Layer 2 broadcasts.
 - C. Bridges are frequently faster than switches.
 - D. Switches have a higher number of ports than most bridges.
 - E. Bridges define broadcast domains while switches define collision domains.
 - F. Both bridges and switches make forwarding decisions based on Layer 2 addresses.
9. What are some of the advantages of using a router to segment the network?

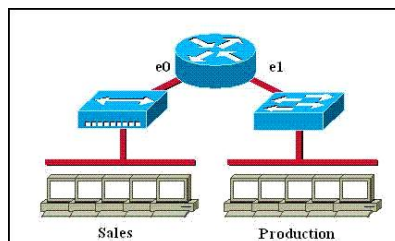
(Choose two.)

- A. Filtering can occur based on Layer 3 information.
 - B. Broadcasts are eliminated.
 - C. Routers generally cost less than switches.
 - D. Broadcasts are not forwarded across the router.
 - E. Adding a router to the network decreases latency.
10. What functions do routers perform in a network? (Choose two.)

- A. packet switching
- B. access layer security
- C. path selection
- D. VLAN membership assignment
- E. bridging between LAN segments
- F. microsegmentation of broadcast domains

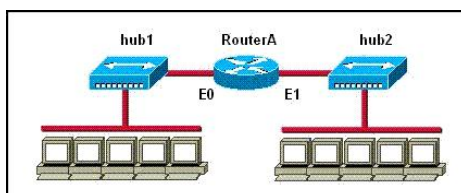
11. Which of the following statements describe the network shown in the graphic?

(Choose two.)

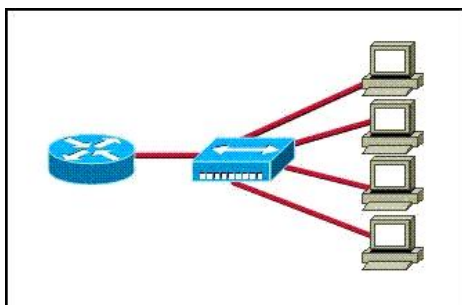


- A. There are two broadcast domains in the network.
 - B. There are four broadcast domains in the network.
 - C. There are six broadcast domains in the network.
 - D. There are four collision domains in the network.
 - E. There are five collision domains in the network.
 - F. There are seven collision domains in the network.
12. Refer to the graphic. How many collision domains are shown?

- A. one
- B. two
- C. three
- D. four
- E. six
- F. fourteen



13. Refer to the exhibit. What two results would occur if the hub were to be replaced with a switch that is configured with one Ethernet VLAN? (Choose two.)



- A. The number of collision domains would remain the same.
- B. The number of collision domains would decrease.
- C. The number of collision domains would increase.
- D. The number of broadcast domains would remain the same.
- E. The number of broadcast domains would decrease.
- F. The number of broadcast domains would increase.

14. Which of the following are associated with the application layer of the OSI model?

(Choose two.)

- A. ping
- B. Telnet
- C. FTP
- D. TCP
- E. IP

15. At which OSI layer is a logical path created between two host systems?

- A. session
- B. transport
- C. network
- D. data link
- E. physical

16. Why does the data communication industry use the layered OSI reference model?

(Choose two.)

- A. It divides the network communication process into smaller and simpler components, thus aiding component development, design, and troubleshooting.
- B. It enables equipment from different vendors to use the same electronic components, thus saving research and development funds.
- C. It supports the evolution of multiple competing standards, and thus provides business opportunities for equipment manufacturers.
- D. It encourages industry standardization by defining what functions occur at each layer of the model.
- E. It provides a means by which changes in functionality in one layer require changes in other layers.

17. An inbound access list has been configured on a serial interface to deny packet entry for TCP and UDP ports 21, 23 and 25. What types of packets will be permitted by this ACL? (Choose three.)

- A. FTP B. Telnet C. SMTP
D. DNS E. HTTP F. POP3

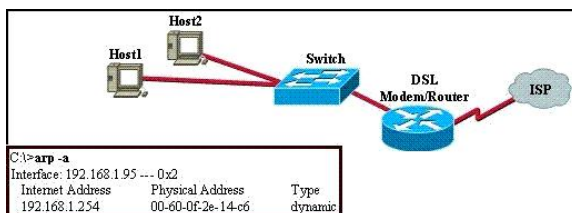
18. DNS servers provide what service?

- A. Given an IP address, they determine the name of the host that is sought.
B. They convert domain names into IP addresses.
C. They run a spell check on host names to ensure accurate routing.
D. They map individual hosts to their specific IP addresses.

19. For security reasons, the network administrator needs to prevent pings into the corporate networks from hosts outside the internetwork. Which protocol should be blocked with access control lists?

- A. IP B. ICMP C. TCP D. UDP

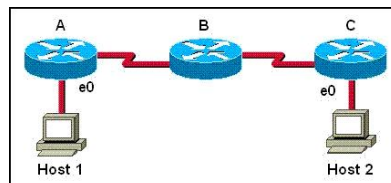
20. The user of Host1 wants to ping the DSL modem/router at 192.168.1.254. Based on the Host1 ARP table that is shown in the exhibit, what will Host1 do?



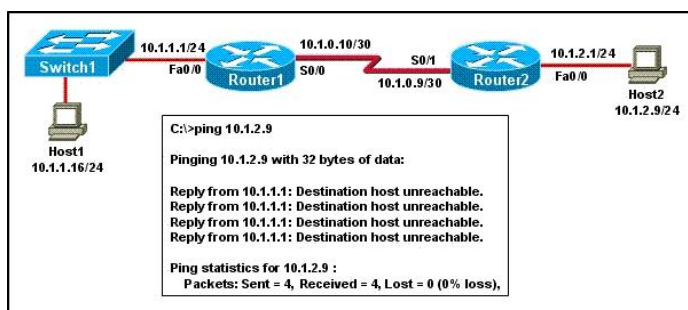
- A. send a unicast ARP packet to the DSL modem/router
B. send unicast ICMP packets to the DSL modem/router
C. send Layer 3 broadcast packets to which the DSL modem/router responds
D. send a Layer 2 broadcast that is received by Host2, the switch, and the DSL modem/router
21. Host 1 is trying to communicate with Host 2.

The e0 interface on Router C is down. Which of the following are true? (Choose two.)

- A. Router C will use ICMP to inform Host 1 that Host 2 cannot be reached.
B. Router C will use ICMP to inform Router B that Host 2 cannot be reached.
C. Router C will use ICMP to inform Host 1, Router A, and Router B that Host 2 cannot be reached.
D. Router C will send a Destination Unreachable message type.
E. Router C will send a Router Selection message type.
F. Router C will send a Source Quench message type.



22. Refer to the exhibit. A network administrator attempts to ping Host2 from Host1 and receives the results that are shown. What is a possible problem?



- A. The link between Host1 and Switch1 is down.
- B. TCP/IP is not functioning on Host1.
- C. The link between Router1 and Router2 is down.
- D. The default gateway on Host1 is incorrect.
- E. Interface Fa0/0 on Router1 is shutdown.
- F. The link between Switch1 and Router1 is down.

23. What is the purpose of an ARP request message?

- A. It binds the IP address of a host to the network that it is on.
- B. It builds a correlation between an IP address and a MAC address.
- C. It provides connectivity and path selection between hosts on a network.
- D. It encapsulates the Layer 3 address and then passes the packet to Layer 2.
- E. It creates a session by passing a header with the destination Layer 2 address to the transport layer.

24. An administrator issues the command ping 127.0.0.1 from the command line prompt on a PC. If a reply is received, what does this confirm?

- A. The PC has connectivity with a local host.
- B. The PC has connectivity with a Layer 3 device.
- C. The PC has a default gateway correctly configured.
- D. The PC has connectivity up to Layer 5 of the OSI model.
- E. The PC has the TCP/IP protocol stack correctly installed.

25. Acknowledgements, sequencing, and flow control are characteristics of which OSI layer?

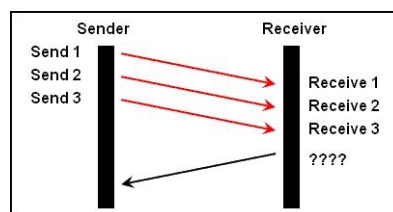
- A. Layer 2
- B. Layer 3
- C. Layer 4
- D. Layer 5
- E. Layer 6
- F. Layer 7

26. Which of the following are types of flow control? (Choose three.)

- A. buffering
- B. cut-through
- C. windowing
- D. congestion avoidance
- E. load balancing

27. A TCP/IP transfer is diagrammed in the exhibit.

A window size of three has been negotiated for this transfer. Which message will be returned from the receiver to the sender as part of this TCP/IP transfer?



- A. send ACK 1-3 B. send ACK 3 C. send ACK 4
D. send ACK 4-6 E. send ACK 6 F. send ACK 7

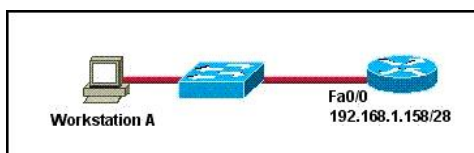
28. Which of the following describe private IP addresses? (Choose two.)

- A. addresses chosen by a company to communicate with the Internet
B. addresses that cannot be routed through the public Internet
C. addresses that can be routed through the public Internet
D. a scheme to conserve public addresses
E. addresses licensed to enterprises or ISPs by an Internet registry organization

29. If an ethernet port on a router was assigned an IP address of 172.16.112.1/20, what is the maximum number of hosts allowed on this subnet?

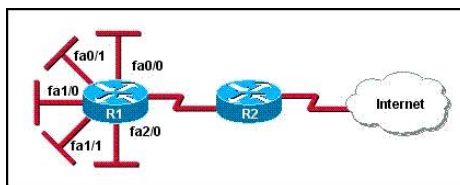
- A. 1024 B. 2046 C. 4094
D. 4096 E. 8190

30. Refer to the exhibit. What IP address should be assigned to Workstation A?



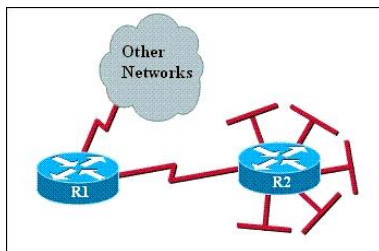
- A. 192.168.1.143/28 B. 192.168.1.144/28 C. 192.168.1.145/28
D. 192.168.1.159/28 E. 192.168.1.160/28

31. The Ethernet networks connected to router R1 in the graphic have been summarized for router R2 as 192.1.144.0/20. Which of the following packet destination addresses will R2 forward to R1, according to this summary? (Choose two.)



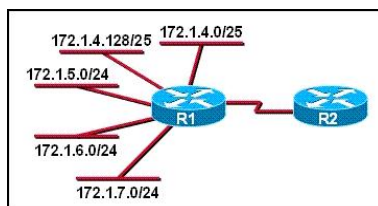
- A. 192.1.159.2 B. 192.1.160.11 C. 192.1.138.41
D. 192.1.151.254 E. 192.1.143.145 F. 192.1.1.144

32. Refer to the exhibit. The networks connected to router R2 have been summarized as a 192.168.176.0/21 route and sent to R1. Which two packet destination addresses will R1 forward to R2? (Choose two.)



- A. 192.168.194.160 B. 192.168.183.41 C. 192.168.159.2
D. 192.168.183.255 E. 192.168.179.4 F. 192.168.184.45

33. Refer to the exhibit. What is the most efficient summarization that R1 can use to advertise its networks to R2?



- A. 172.1.0.0/22 B. 172.1.0.0/21 C. 172.1.4.0/22
D. 172.1.4.0/24 E. 172.1.4.0/25
172.1.5.0/24 172.1.4.128/25
172.1.6.0/24 172.1.5.0/24
172.1.7.0/24 172.1.6.0/24
172.1.7.0/24

34. Refer to the exhibit. The partial frame shown in the exhibit displays select header information as it arrives at the destination host. Which graphic represents the correct header information in the responding frame returned to the remote host?

Destination	Source	Destination	Source	Destination	Source	S Y N K
000d.56ad.a313	000a.8a47.e612	192.168.14.1	192.168.14.2	23	42335	1 0

A.

Destination	Source	Destination	Source	Destination	Source	S Y N K
000a.8a47.e612	000d.56ad.a313	192.168.14.2	192.168.14.1	23	42335	0 1

B.

Destination	Source	Destination	Source	Destination	Source	S Y N K
000a.8a47.e612	000d.56ad.a313	192.168.14.2	192.168.14.1	23	42336	1 1

C.

Destination	Source	Destination	Source	Destination	Source	S Y N K
000d.56ad.a313	000a.8a47.e612	192.168.14.1	192.168.14.2	42335	23	0 1

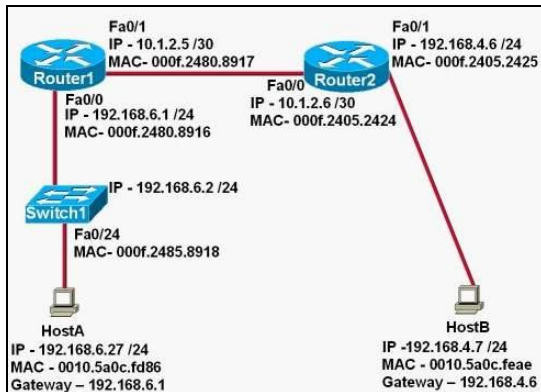
D.

Destination	Source	Destination	Source	Destination	Source	S Y N K
000a.8a47.e612	000d.56ad.a313	192.168.14.2	192.168.14.1	42335	23	1 1

E.

Destination	Source	Destination	Source	Destination	Source	S Y N K
000d.56ad.a313	000a.8a47.e612	192.168.14.2	192.168.14.1	42336	23	0 0

35. Refer to the exhibit. After HostA pings HostB, which entry will be in the ARP cache of HostA to support this transmission?



C. A.

Interface Address	Physical Address	Type
192.168.4.7	000f.2480.8916	dynamic

C. B.

Interface Address	Physical Address	Type
192.168.4.7	0010.5a0c.fea6	dynamic

C. C.

Interface Address	Physical Address	Type
192.168.6.1	0010.5a0c.fea6	dynamic

C. D.

Interface Address	Physical Address	Type
192.168.6.1	000f.2480.8916	dynamic

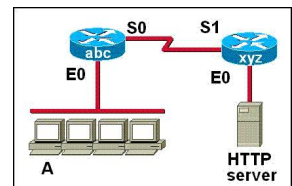
C. E.

Interface Address	Physical Address	Type
192.168.6.2	0010.5a0c.fea6	dynamic

C. F.

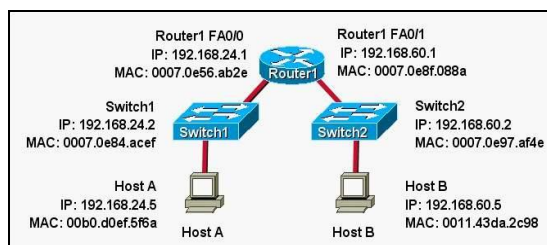
Interface Address	Physical Address	Type
192.168.6.2	000f.2485.8918	dynamic

36. Refer to the graphic. Host A has established a connection with the HTTP server attached to interface E0 of the xyz router. Which of the following statements describe the information contained in protocol data units sent from host A to this server? (Choose three.)



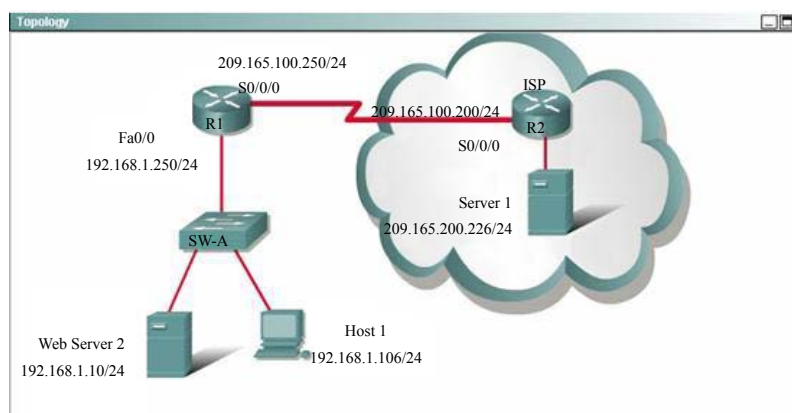
- A. The destination port number in a segment header will have a value of 80.
- B. The destination port number in a segment header will have a unique value greater than or equal to 1023.
- C. The destination address of a frame will be the MAC address of the HTTP server interface.
- D. The destination address of a frame will be the MAC address of the E0 interface of the abc router.
- E. The destination IP address of a packet will be the IP address of the E0 interface of the abc router.
- F. The destination IP address of a packet will be the IP address of the network interface of the HTTP server.

37. Refer to the exhibit. What is the correct addressing for a frame and packet received by Host B from Host A?



- | | |
|---|---|
| <p>A. Destination MAC: 0011.43da.2c98
Source MAC: 0070.0e8f.088a
Destination IP: 192.168.60.5
Source IP: 192.168.24.5</p> <p>C. Destination MAC: 0011.43da.2c98
Source MAC: 0070.0e8f.088a
Destination IP: 192.168.60.5
Source IP: 192.168.60.1</p> | <p>B. Destination MAC: 0011.43da.2c98
Source MAC: 00b0.d0ef.5f6a
Destination IP: 192.168.60.5
Source IP: 192.168.24.5</p> <p>D. Destination MAC: 0011.43da.2c98
Source MAC: 0070.0e97.af4e
Destination IP: 192.168.60.5
Source IP: 192.168.60.2</p> |
|---|---|

38. Host 1 sends a request for a file to remote sever1. Which destination address does Host 1 place f the packet containing the request? (题 38~42 均使用本题中的图)



- A. The Mac address of the NIC in Sever1.
- B. The IP address of Server 1.
- C. The MAC address of the s0/0/0 interface of router R2.
- D. The IP address of the s0/0/0 interface of router R1.
- E. The IP address of the Fa0/0 interface of router R1.

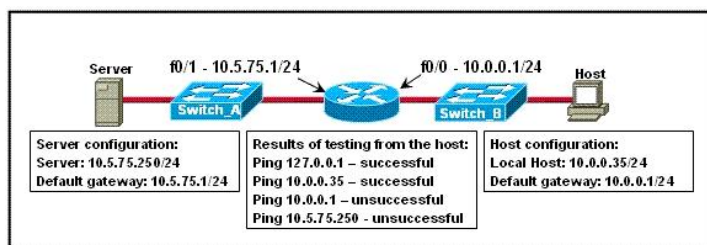
39. Host 1 sends an ICMP echo request to remote server1. Which destination address does Host 1 place in the Layer2 header of the frame containing the ping packet?

- A. The IP address of server 1.
- B. The MAC address of NIC in server 1.
- C. The IP address of F0/0 interface of router R1.
- D. The MAC address of the Fa0/0 interface of router R1.
- E. The IP address of the s0/0/0 interface of router R2.
- F. The MAC address of the s0/0/0 interface of router R2.

40. R1 forwards a packet from Host 1 to remote Server 1. Which statement describes the use of a MAC as the frame carrying this packet leaves the s0/0/0 interface of R1?

- A. The frame does not have MAC addresses.
- B. The source MAC address in the frame is the MAC address of the NIC of Host 1.
- C. The source MAC address in the frame is the MAC address of the s0/0/0 interface of R1.

- D. The destination MAC address in the frame is the MAC address of the NIC of server 1.
 E. The destination MAC address in the frame is the MAC address of the s0/0/0 interface of R2.
41. Host 1 receives a file from remote server 1. Which MAC address appears as the source address in the header of the frames received by Host 1?
- A. The MAC address of the NIC in Host 1 .
 B. The MAC address of the NIC in server 1.
 C. The MAC address of the Fa0/0 interface of router R1.
 D. The MAC address of the s0/0/0 interface of the router R2.
42. Host 1 has just started up and requests a web page from web server 2. Which two statements describe steps in the process Host 1 uses to send the request to web server 2 (choose two)?
- A. Host 1 addresses the frames to the MAC address of router R1.
 B. Host 1 looks in its ARP cache for the MAC address of router R1.
 C. Host 1 addresses the frames to the MAC address of web server 2.
 D. Host 1 sends the packets to router R1 to be forwarded to web server 2.
 E. Host 1 sends a broadcast ARP request to obtain the MAC address of webserver2.
43. A receiving host computes the checksum on a frame and determines that the frame is damaged. The frame is then discarded. At which OSI layer did this happen?
- A. session B. transport C. network
 D. data link E. physical
44. While troubleshooting a network connectivity problem, a technician observes steady link lights on both the workstation NIC and the switch port to which the workstation is connected. However, when the ping command is issued from the workstation, the output message "Request timed out." is displayed. At which layer of the OSI model does the problem most likely exist?
- A. the session layer B. the protocol layer C. the data link layer
 D. the access layer E. the network layer F. the application layer
45. Refer to the exhibit. A technician is troubleshooting a host connectivity problem. The host is unable to ping a server connected to Switch_A. Based on the results of the testing, what could be the problem?



- A. A remote physical layer problem exists.
 B. The host NIC is not functioning.
 C. TCP/IP has not been correctly installed on the host.

D. A local physical layer problem exists.



2.8 真题解答***

1. 解：DE

题目问：在哪两种拓扑中使用了正确类型的双绞线（选 2 个）？这是一个考双绞线类型和应用场合的题目，在 2.1.3 节中介绍到双绞线有 3 种类型：直通线（Straight-through），用于不同种设备的互连；交叉线（Crossover），用于同种设备的互连；全反线（Rollover），主要用于对路由器和交换机进行初始配置，在本书后面的路由器和交换机初始配置中，读者将会使用这种线缆，连接计算机的 COM（串行通信端）口和路由器或交换机的 Console（控制台）端口。此外，计算机和路由器属于同种设备，交换机和集线器也属于同种设备。虽说新款交换机或路由器能自动识别所接设备的类型，并调整接口状态，自动适应线缆的类型。但在 CCNA 考试中，默认没有使用支持智能接口的设备。正确解答此题，还要注意连接路由器或交换机的端口类型，是以太网还是配置端口，譬如 C 选项中连接的就是配置端口（Console0 可以简写成 con0）。基于以上分析，路由器和交换机间应使用直通线，而 A 答案中使用的却是交叉线，故 A 错；计算机和交换机间应使用直通线，而 B 答案中使用的却是交叉线，故 B 错；计算机对路由器进行初始配置，应使用全反线连接计算机的 COM 口和路由器的 Console 口，而 C 答案中使用的却是交叉线，故 C 错；两台交换机间应使用交叉线，故 D 正确；计算机和路由器属于同种设备，应使用交叉线，故 E 也正确。

2. 解：D

题目问：圣何塞市（美国城市）的一个小公司，有两幢建筑需要通过以太网互连，要求带宽至少是 100Mbps。两幢建筑的电压不一样，布线时要考虑这一情况，问下面的哪一种传输介质将被使用？如果从传输距离上看，非屏蔽双绞线（UTP）、屏蔽双绞线（STP）、同轴电缆（coaxial）、光纤（fiber optic）均可满足传输要求。但考虑到是室外布线，且传输速度至少要 100Mbps，且两端的电压不同，这样铜质线缆就不能满足要求。而光纤传输速率高，可达数千兆 bps；抗干扰性强，不会受到电磁干扰；且不会因为雷击而损坏两端的设备。故正确答案选 D，使用光纤。

3. 解：C

题目问：参照图，Switch1 刚刚完成重启和自检程序。计算机 A 发送它的初始数据帧到计算机 C。有关组建交换表（也就是交换机的 MAC 地址表）方面，交换机将要做的第一件事情是什么？本章 2.3.2 节介绍了网桥和交换机的工作原理，根据源 MAC 地址进行学习，构建交换机的 MAC 地址表，交换机的 MAC 地址表保存在 RAM，断电全部丢失。题目中提到交换机刚刚重启，暗示了交换机的 MAC 地址表为空，当计算机 A 发往计算机 C 的数据帧到达交换机 1 时，交换机要做的第一件事情就是数据帧中的源 MAC 地址进行学习，把计算机 A 的 MAC 地址添加进 MAC 地址表，也就是这里说的交换表。故正确答案选择 C。交换机的交换表是 MAC 地址表，根本不会添加 IP 地址，故 A 和 B 错误。计算机 C 的 MAC 地址是数据帧的目的 MAC 地址，交换机 1 要根据目的 MAC 地址进行转发，因为交换机 1 的 MAC 地址表中目前还没有学到计算机 C 的 MAC 地址，交换机 1 将会泛洪（也就是广播式转发，向除接收端口以外的所有端口转发）该数据帧。题目中虽没有这一问，但

考生还是应该知道的。

4. 解: B

题目问: 参照图, 交换机 1 需要发送数据到一台 MAC 地址为 00b0.d056.efa4 的计算机, 问交换机将对这个数据帧做什么? 此题考的还是交换机工作原理, 本书后面会介绍到“show mac-address-table”命令用于查看交换机的 MAC 地址表, 从图中可以看出, 交换机的 MAC 地址表中并没有 MAC 地址 00b0.d056.efa4。本章 2.3.2 节介绍交换机的转发情况分为三种, 即交换机对未知的单播帧、组播帧和广播帧, 采用的都是泛洪的方式, 即发往除接收到这个数据的端口以外的所有端口。所以, 选 B。

5. 解: C

题目问: 交换机为什么永远学不到广播地址? 首先要知道交换机是根据源 MAC 地址进行学习的, 它将收到的数据帧的源 MAC 地址和收到的这个端口进行绑定, 形成一个条目放入 MAC 地址表中。所谓数据帧的源 MAC 地址也就是发出这个数据帧的设备的 MAC 地址, 没有设备的 MAC 地址是“FFFFFFFFFFFF”, 所以交换机当然学习不到广播的 MAC 地址。

6. 解: B

题目问: 如果以太网交换机收到一个单播帧, 并且单播帧的目的 MAC 地址已经在交换机的交换表中, 交换机将做什么? 本章 2.3.2 节, 介绍过交换机对已知目的 MAC 地址的单播帧将只往对应的端口转发, 即交换机交换表中与该目的 MAC 地址对应的端口转发。

7. 解: E

题目问: 考虑到使用交换机和集线器进行互连, 下面哪一个说法是正确的? A 选项说交换机对数据帧花费的处理时间比集线器少, 也就是说, 交换机对数据帧的处理速度比集线器快。这种说法是不正确的, 集线器是物理层设备, 只能简单地对比特流进行放大转发; 而交换机除了完成集线器完成的物理层功能外, 还需要学习数据帧的源 MAC 地址, 并查询数据帧的目的 MAC 地址, 有时还需要检验数据帧没有错误后, 再进行转发, 所以交换机对数据包的处理时间比集线器要长。因为路由器对数据包的处理比交换机还要复杂, 所以路由器对数据包的处理时间比交换机要长, 比集线器更长。B 选项说交换机不转发广播, 这种方法也是错误的, 交换机对广播进行的是泛洪处理, 交换机不能阻止广播, 本书后面章节还会介绍到 STP (Spanning Tree Protocol, 生成树协议), 用来阻止交换的网络中因为冗余路径而形成的广播风暴。路由器是可以用来隔离广播的。选项 C 说集线器可以用来过滤帧也是错误的, 集线器工作在物理层, 只能处理比特流; 而数据帧处在数据链路层, 处在低层的集线器无法识别, 更不能过滤处在高层的数据帧。选项 D 说使用集线器可以增加主机使用的带宽也是错误的, 处在集线器互连网络中的所有主机同时只能有一台主机发送数据包, 不然就会形成冲突, 造成发送失败, 且集线器只能工作在半双工模式下, 即收和发不能同时进行, 每台主机的可用带宽更少。使用交换机可以增加每台主机的可用带宽。交换机不仅可以根据 MAC 地址过滤, 且可以工作在全双工的模式下, 即收和发可以同时进行。选项 E 说交换机增加了冲突域的数量是正确的, 交换机每一个端口就是一个冲突域, 而所有集线器互连的网络是一个冲突域。

8. 解: BDF

题目问: 关于网桥和交换机, 下面哪一种说法是正确的 (选 3 个)? 本章 2.3.2 节提到了

网桥和交换机的区别，二者都工作在 OSI 的第二层，即数据链路层，工作原理类似，都是基于数据帧的源 MAC 地址（即第二层地址，第三层地址指的是 IP 地址）进行学习，基于目的 MAC 地址进行转发，都能用来隔离冲突域，但不能用来隔离广播，都转发二层的广播，属于同一个广播域。但二者也有区别，网桥一般只有两个端口，而交换机有更多的端口；网桥基于软件，而交换机基于硬件，故交换机有更快的转发速度。故正确答案选择 B、D 和 F。

9. 解：AD

题目问：用路由器来分割一个网络的好处是什么（选 2 个）？路由器工作在第三层，即网络层的设备，可以基于三层的信息来实现过滤，故 A 正确；路由器是可以隔离广播的，阻止广播从一个广播域中传播到另一个广播域中，但它是没有办法消除广播的，故 B 错；一般路由器的价格普遍比交换机贵，而不是便宜，故 C 错；广播不能通过路由器被转发，故 D 正确；增加路由器在网络中将会增加延迟，前面已经介绍过，路由器的延迟大于交换机，交换机的延迟大于集线器，故 E 错。

10. 解：AC

题目问：路由器在网络中执行什么功能（选 2 个）？路由器在网络中主要执行的功能是包交换和路径选择，路径选择可以选择正确的路径，然后把数据包交换到对应的端口。故 A 和 C 正确。B 选项提到接入层的安全，接入层的安全一般都是在接入层交换机上实现的。D 选项提到 VLAN 成员关系的分配，VLAN 也是在交换机上配置的，而不是路由器。E 选项提到桥接局域网段，路由器在局域网段间执行的是路由而不是桥接。F 选项提到微分广播域，这不太现实，路由器可以用来分隔广播域，但微分的工作量较大，成本较高。故只有 A 和 C 正确。此题直接选择正确的答案更容易，如果学完全书再做此题，相对要容易很多。

11. 解：AF

题目问：下面哪一个语句描述了图中的网络（选 2 个）？这一题问的是广播域和冲突域的问题，涉及的网络设备有集线器、交换机和路由器、集线器处于物理层，所有接口同属于一个冲突域、一个广播域；交换机处于在数据链路层，每个接口是一个单独的冲突域，非 VLAN 型交换机的所有端口属于同一个广播域，如果是 VLAN 型交换机，每个 VLAN 是一个广播域；路由器处于网络层，每个端口是一个单独的冲突域，也是一个单独的广播域。图中路由器左边是一个广播域，也是一个冲突域；路由器右边有一个广播域，因为交换机上只接了一个部门，说明只有一个 VLAN。交换机有 5 个端口连接 Production 部门，1 个端口连接路由器，因为交换机每个端口就是一个冲突域，所以右边有 6 个冲突域。整个网络中有 2 个广播域、7 个冲突域。

12. 解：B

题目问：参照图，图中有多少个冲突域？根据上一题的解释，路由器左边有 1 个冲突域，右边有 1 个冲突域，共有 2 个冲突域，如果问到广播域的数量，也是 2 个。

13. 解：CD

题目问：参照图，如果 HUB 被一台只配置了一个以太网 VLAN 的交换机替代，哪两个结果将发生（选 2 个）？因为交换机上只配置了一个 VLAN，所以广播域的数据量不会发生变化。本来是集线器相连 4 台计算机和 1 台路由器的，只有一个冲突域，如果换成交换

机互连，将有 5 个冲突域，即交换机每一个端口都是一个独立的冲突域。故正确答案选 C（冲突域的数量增加）和 D（广播域的数量不变）。

14. 解：BC

题目问：下面哪一个是与 OSI 模型的应用层相关的（选 2 个）？其实题目问的就是哪一个是应用层协议，根据本章 2.3.7 节的叙述，很容易就可以选出 B 和 C。ping 和 IP 属于网络层协议，TCP 属于传输层协议。

15. 解：C

题目问：在 OSI 模型的哪一层，两台主机系统建立了一条逻辑路径？MAC 地址是物理地址，IP 地址是逻辑地址，两台主机系统通过 IP 地址建立的连接称为逻辑路径，而 IP 地址处在网络层，故正确答案选 C。

16. 解：AD

题目问：为什么工业数据通信使用分层的 OSI 参考模型（选 2 个）？这一题简直就是考大家的英文水平，A 选项说 OSI 参考模型把网络通信处理划分成小的和简单的部分，这样每一个小的部分都更容易发展、设计和故障排除，A 是正确的；B 选项说 OSI 参考模型使用不同厂商都使用相同的电子组件，节省了开发和研究基金，该选项错，OSI 并没有规定使用什么样的硬件；C 选项说 OSI 模型支持多个有竞争的标准，因此给设备制造商提供更多的商业机会，该选项错，OSI 参考模型的推出，就是想提供一个统一的标准，以便不同厂商生产的设备之间可以协同工作；D 选项说 OSI 参考模型通过定义发生在模型每一层的功能来加速工业的标准化，正确；E 选项说 OSI 提供了一种方法，改变一层功能时要求其他层也跟着改变，该选项错，分层的目的就是为了使层和层之间相对独立，改变一层的功能不至于影响到其他各层。

17. 解：DEF

题目问：一个入方向的访问控制列表被配置在一个串行口上，目的是拒绝去往 TCP 和 UDP 的端口 21、23 和 25，什么类型的包将会被这个 ACL 允许？本题虽提到了访问控制列表，但真正的考点，还是考大家对常用协议的掌握。有些常用的公用端口号是需要记住的：FTP（TCP 的 20 和 21）、Telnet（TCP 的 23）、SMTP-E-mail（TCP 的 25）、DNS（TCP 和 UDP 的 53）、TFTP（UDP 的 69）、HTTP（TCP 的 80）、POP3（TCP 的 110）。在这里，过滤了端口号为 21、23 和 25 的端口的流量，因此就是过滤了 FTP、Telnet 和 SMTP 的流量，剩下的就是可以允许的。故 D、E 和 F 正确。

18. 解：B

题目问：DNS 提供了什么样的服务？DNS 提供的是域名解析服务，即把域名解析为对应的 IP 地址，譬如把南京工业大学的域名 www.njut.edu.cn 解析成 IP 地址 202.119.248.65。故正确答案选 B。

19. 解：B

题目问：出于安全方面的考虑，网络管理员需要阻止外部网中的主机 ping 公司的内部网络，哪一个协议将被访问控制列表阻止？ping 命令利用 ICMP 协议的 echo 和 echo-replay 两个报文来检测链路是否连通。所以如果要阻止 ping 的流量到网络，只要过滤掉 ICMP 协

议的报文就可以了。

20. 解: B

题目问: Host1 想 ping 路由器的 IP 地址 192.168.1.254, 基于图中显示的 Host1 的 ARP 表, Host1 将做什么? 参照本章 2.4.2 节, 如果计算机的 ARP 表中已经有了目的计算机的缓存项, 则直接封装, 发送出去, 这是一个单播包; 如果没有, 则发送 ARP 的查询包, 这是一个二层的广播包。图中可以看到 Host1 的 ARP 缓存中已经有 192.168.1.254 的缓存项, 则 Host1 直接封装目的 MAC 地址和目的 IP 地址, 是一个单播包。

21. 解: AD

题目问: Host1 试图和 Host2 通信, 但路由器 C 的 E0 口 DOWN 掉, 下面哪一种说法是正确的 (选 2 个)? 路由器 C 连接 Host2 的接口 E0 DOWN 了, 那么最直接的反映就发生在路由器 C 上, C 的路由表中的这个条目消失了, 因此当 Host1 想要跟 Host2 建立连接的时候, 路由器 C 就发送一个目的网段不可达的消息; 如果是使用 ping 命令, 那么 Router C 就使用 ICMP 的包文告诉 Host1, Host2 是不可达的, 并不会告诉中间的路由设备。想象一下在路由器 C 收到的 IP 报文中也没有中间设备的 IP 地址, 路由器 C 是无法通知到中间网络设备的。

22. 解: C

题目问: 参照图, 一个网络管理员尝试从主机 1 ping 主机 2, 测试的结果如图中所示, 可能是什么问题? 从图中的输出可以看出信息是从路由器 1 返回的, 提示“目的主机不可达”, 这至少说明一点, 从 Host1 到路由器的链路正常, 那么 A 错误; 既然可以 ping, 说明 TCP/IP 协议已经安装, 且工作正常, 那么 B 错误; 如果 Host1 网关配置错误, Host1 将会把数据包转发到一个错误的地址上, 既然是转发到错误的地址上, 路由器 1 就不会对此做出反应, 既然路由器 1 给予应答, 说明 Host1 的网关配置正确, 那么 D 错误; 如果路由器 1 的 Fa0/0 被关闭, Host1 应该是找不到网关, 收到的提示应该是“Request time out”, 那么 E 错误; 如果交换机 1 和路由器 1 之间的链路有问题, Host1 也找不到网关, 收到的提示也是“Request time out”, 那么 F 错误; 只有 C 答案正确, Host1 把数据包转发到路由器 1, 可是因为路由器 1 与路由器 2 之间的链路故障, 路由器 1 上没有去往 10.1.2.9 的路由, 路由器 R1 才会发消息通知源设备, 目的不可达。如果路由器 1 和路由器 2 之间的链路正常, 但路由器 R1 上没有配置正确的路由, 也会收到这种提示。如果路由器 1 把数据包转发到路由器 2 上, 但路由器 2 上没有正确的路由, Host1 上看到的消息将是“Reply from 10.1.0.9: Destination host unreachable.”。

23. 解: B

题目问: ARP 查询包的目的是什么? 根据本章 2.4.2 节的介绍, 大家知道 ARP 查询包是一个二层的广播包, 其作用是已知目标设备的 IP 地址, 查询目标设备的 MAC 地址。B 选项说是构造 IP 地址和 MAC 地址间的相互关系, 只有这个答案最接近。

24. 解: E

题目问: 一个网络管理员在 PC 的命令行模式下, 执行“ping 127.0.0.1”, 如果收到应答消息, 可以确认什么? IP 地址 127.0.0.0/8 是一个私有的保留地址段, 该地址段中的任何一个 IP 地址都是回环地址, 一般用于测试, 测试 TCP/IP 协议栈是否起来了。在一台 PC 上

能 ping 通 127.0.0.0/8 网段的地址，说明这个 PC 的 TCP/IP 协议栈是正确安装的。

25. 解：C

题目问：确认、序列号和流控是 OSI 模型哪一层的特点？本章介绍的 TCP 协议通过使用确认重传机制保证数据传输的可靠性，TCP 协议使用了序列号和确认号，同时还提供了流控功能。TCP 协议处在 OSI 模型的第 4 层，即传输层。

26. 解：ACD

题目问：下面哪一个是流控的类型（选 3 个）？快速转发（cut-through）、负载均衡（load balancing）与流量控制无关。而缓存技术，可以缓存一定量的过量的数据包，加快发送速度；TCP 协议的滑动窗口机制，可以动态调整窗口的大小，调整每次发送可以发送的字节数；拥塞避免可以根据链路忙闲情况，调整发送的速率。缓存、窗口机制和拥塞避免都起到流控的作用。

27. 解：C

题目问：参照图，接收者和发送者以协商好的窗口大小 3 发送数据，根据图中的显示和 TCP/IP 传输的特点，接收者将返回什么信息给发送者？从图中可以看出发送者发送了 3 个字节给接收者，而前提条件中又提到了，发送者和接收者已经协商好窗口的大小是 3，所以接收者可以正常接收这 3 个字节，那么接收者将发回 ACK 4，表示期望接收的下一个字节编号是 4，也暗示了前面 3 个字节被正常接收。

28. 解：BD

题目问：下面哪一个描述了私有 IP 地址（选 2 个）？私有 IP 地址是不能在公网上传递的。IPv4 地址越来越短缺，为了解决这个问题，可以在局域网内使用私有地址，如果一个使用私有地址的设备需要同外网通信，可以通过 NAT 将这个私有地址转换为公有地址，这样不仅可以节省公网地址，还可以达到隐藏内部地址的目的。选项 A、C 和 E 描述的都是公网地址的特征。

29. 解：C

题目问：如果一台路由器的以太网端口被分配了一个 IP 地址 172.16.112.1/20，那么这个子网最大允许容纳多少台主机？接在这个子网中，网络位有 20 位，主机位有 12 位，可以容纳的主机数是 $2^{12}-2=4094$ 台，如果有 4093 就是更合适的选项，因为 4094 还要减去被路由器接口占用的一个地址。

30. 解：C

题目问：参照图，工作站 A 将被分配哪一个 IP 地址？图中给出了路由器局域网接口的 IP 地址 192.168.1.158/28，只要工作站 A 的 IP 地址与路由器接口在同一个子网中即可，但不能是子网地址或子网广播地址。利用本章 2.5.5 节例 2 中的方法二，192.168.1.158/28 的主机位有 4 位，每个子网中可以容纳的 IP 数量是 16 个，被划分子网的 IP 地址分配如下：

192.168.1.0~15

192.168.1.16~31

192.168.1.32~47

...

192.168.1.128~143

192.168.1.144~159

...

192.168.1.240~255

每一行前面的 IP 地址是该子网的网络号，后面的 IP 地址是该子网的广播地址，都不能使用。158 落在 192.168.1.144/28 子网内，该子网可用的 IP 地址从 145~158，只有 C 选项正确。

31. 解：AD

题目问：连接在路由器 R1 上的以太网被汇总成 192.1.144.0/20 传给 R2，根据汇总路由，下面的哪一个数据包目的地址将被路由器 R2 转发到 R1（选 2 个）？只要目的 IP 地址在 192.1.144.0/20 子网中的数据包都将被路由器 R2 转发到 R1。首先要算出 192.1.144.0/20 子网中的 IP 地址范围，该子网的网络位有 20 位，主机位有 12 位，把主机位全部设成 1 就是广播地址，也是该子网中的最后一个 IP 地址，该 IP 地址是 192.1.144.0 加上最后 12 位的 1，也就是 $192.1.144.0 + 0.0.15.255 = 192.1.159.255$ 。落在该子网范围（192.1.144.0~192.1.159.255）内的 IP 地址有选项 A 和 D。

32. 解：BE

题目问：参照图，连接到 R2 的网络已经被汇总成 192.168.176.0/21 并发送到 R1，哪两个目的地址的数据包将被 R1 转发到 R2（选 2 个）？此题与前一题相同，根据 21 位的掩码位数可以推断在第 3 个 8 字节的前 5 位是相同的，不同的是后面的 3 位，而将 176 写成二进制的形式为 10110000，网络号是最小的 IP 地址，广播地址是最大的 IP 地址，即 10110111，转换成十进制数是 183。则 IP 子网中的 IP 地址范围是 192.168.176.0~192.168.183.255，可以看出 B 和 E 落在此区间内。D 选项是该子网的广播，路由器 R1 根据路由表也可以判断出这是一个广播地址，在默认情况下，路由器不转发广播包，也就是说，路由器 R1 不转发去往 192.168.183.255 的数据包到路由器 R2。

33. 解：C

题目问：参照图，哪一种 R1 为了向 R2 通告路由而进行的最有效的汇总？这还是一个关于汇总的问题。要求 R1 将所有的网段用汇总的条目发送给 R2。可以借鉴本章 2.5.5 节例 3 的方法进行汇总，这里首先把 172.1.4.0/25 和 172.1.4.128/25 进行汇总，因为这两个子网的前 24 位都相同，就不用换算成二进制形式了，汇总方法如下：

172.1.4.00000000

172.1.4.10000000

取出共同的部分和对应的位数，就是 172.1.4.0/24，然后再把 172.1.4.0/24，172.1.5.0/24、172.1.6.0/24、172.1.6.0/24 进行汇总，考虑到这 4 个条目的网络位相同，都是 172.1，所以在这里需要汇总的只是第 3 个 8 位，将 4，5，6，7 写成二进制的形式，然后找出相同的位数。

00000100

00000101

00000110

00000111

取出共同的部分和对应的位数，就是 172.1.4.0/22，所以 R1 通告出去汇总的条目为 172.2.4.0/22。这里实现的是最精确的汇总，虽然 B 选项的汇总条目也包括了 R1 上的所有网络，但它是一个不精确的汇总，因为该汇总条目还包括了 172.1.0.0/24、172.1.1.0/24、172.1.2.0/24、172.1.3.0/24 等条目，而题目中明确要求选择最有效的汇总，故 C 最合适。

34. 解：D

题目问：参照图，图中显示的是到达目的主机的帧的部分头部信息，哪一个图表示了回答远程主机的正确的帧的头部信息？问的就是计算机从远程主机收到一个数据帧的头部信息，回应帧的头部信息应该是什么样的。不管两台计算机是否在同一个子网中，接收到帧的源 MAC 地址就是要发回的帧的目的 MAC 地址，接收数据包的源 IP 地址就是要发回数据包的目的 IP 地址，传输层中的源和目的端口也是刚好相反。同时满足 MAC、IP 和端口号的选项只有 D，正确的答案就是 D。如果有两个答案都满足 MAC、IP 和端口号，就需要比较 SYN 位和 ACK 位，本章的图 2-4-8 中提到 TCP 的三次握手建立连接，第一个包只设置 SYN 位，这一点从来源包中可以看到，发回的包中应该设置 SYN 和 ACK 位，选择 SYN 和 ACK 标志都是 1 的选项。应该说这一题出的没水平，既然提到了 SYN 和 ACK，可是不利用这点知识也能选出正确答案。

35. 解：D

题目问：参照图，主机 A ping 主机 B 后，为了支持传输，哪一个条目将出现在主机 A 的 ARP 缓存中？从图中可以看出主机 A 和主机 B 处在不同的子网中，主机 A 发往主机 B 的包，首先要被发往网关。根据本章 2.6 节的知识，主机 A 首先要解析出网关 IP 192.168.6.1 对应的 MAC 地址。所以在主机 A 的 ARP 缓存中应该有网关 IP 对应的条目，也就是 D 答案。没有启用代理 ARP（Proxy-arp）的情况下，计算机的 ARP 缓存中是不会出现不同子网 IP 地址的条目的；即使在使用代理 ARP 的情况下，可以出现不同子网 IP 地址的条目，但这些条目 IP 对应的 MAC 地址却不是远程主机的 MAC 地址，而是开启代理 ARP 功能的路由器本网段接口的 MAC 地址。如果图中的主机 A 没有配置网关，则选项 A 就是正确的选项了，因为 Cisco 路由器默认是启用代理 ARP 功能的。

36. 解：ADF

题目问：参照图，主机 A 已经建立到一台连接在路由器 xyz 以太网 E0 接口上的 HTTP 服务器的连接，下面哪一个语句描述的信息包含在从主机 A 发往服务器的协议数据单元（PDU）中（选 3 个）？HTTP 使用的端口号是 80，因为是从主机 A 发往 HTTP 服务器的，源端口是大于 1023 以上的一个随机端口，目的端口是 80，故 A 选项正确，B 选项错误；数据帧的目的 MAC 地址应该是路由器 abc 的 E0 接口的 MAC 地址，故 C 选项错，D 选项正确；目的 IP 地址应该是服务 HTTP 服务器的 IP 地址，故 E 选项错，F 选项正确。

37. 解：A

题目问：参照图，主机 B 从主机 A 收到的帧和包的地址是多少？掌握本章 2.6 节，可以轻松得出正确答案。来看一下包发送的过程，Host A 发出时，source ip: 192.168.24.5，destination ip: 192.168.60.5，Source mac: 00b0.doef.5f6a，destination mac: 0007.0e56.ab2e；Switch1 收到后经过查找 MAC 地址表，不做任何修改发往 Router 1；Router 1 发出的：source ip 192.168.24.5，destination ip : 192.168.60.5，Source mac : 0007.0e8f.088a，destination

mac:0011.43da.2c98; Switch2 收到后经过查找 MAC 地址表, 不做任何修改发往 Host B。

38. 解: B

题目问: 主机 1 发送一个查询包到远程的文件服务器 1, 主机 1 的查询包中目的地址是哪一个? 不同子网中的主机通信是逻辑地址之间的通信, 即 IP 地址的通信, 并且题目中间的是在“packet”中, 不是在“frame”中, 所以涉及 MAC 地址的选项都可以不用考虑了。从本章 2.6 节的描述中可以知道, 经过不同三层设备时, 第二层的地址不停地被解封装和再封装, 第三层的 IP 地址是不会变的, 因为是发往文件服务器 1 的, 所以目的 IP 地址应该是服务器 1 的。

39. 解: D

题目问: 参照 38 题中的图, 主机 1 发送一个 ICMP 的 echo 请求包到远程服务器 1, 主机 1 在 ping 包的二层帧头部中放置的目的地址是哪一个? 既然是帧的目的地址, 所有涉及 IP 的选项都是错误的。从本章 2.6 节的叙述中, 知道主机 1 首先要把数据发往路由器 R1, 数据帧中的目的 MAC 地址应该是路由器 R1 的 Fa0/0 接口的 MAC 地址。

40. 解: A

题目问: 参照 38 题中的图, 路由器 R1 转发从主机 1 到远程服务器 1 的包, 当这个数据包离开路由器 R1 的 s0/0/0 接口时, 哪一个语句描述了这个数据包中的帧使用的 MAC 地址? MAC 地址是以太网上的地址格式, 路由器 R1 和路由器 R2 之间是串行线路, 串行线路上使用的是封装协议, 没有 MAC 地址。

41. 解: C

题目问: 参照 38 题中的图, 主机 1 从远程文件服务器 1 接收文件, 哪一个源 MAC 地址出现在主机 1 收到的数据帧的头部中? 正确答案是路由器 R1 的 Fa0/0 接口的 MAC 地址。

42. 解: CE

题目问: 参照 38 题中的图, 主机 1 刚刚开机, 从 Web 服务器 webserver2 请求网页, 哪两个语句描述了主机 1 用来发送请求到服务器 webserver2 的过程(选 2 个)? 主机 1 和 Web 服务器在同一个子网中, 两台主机间可以直接通信, 不需要经过路由器, 主机 1 查询本地的 ARP 缓存, 因为主机 1 刚开机, ARP 缓存是空的, 主机 1 发送 ARP 查询包来获得服务器 webserver2 的 MAC 地址, ARP 查询包是以广播形式发送的, 服务器 webserver2 对主机 1 的 ARP 查询包进行应答, 主机 1 获知服务器 webserver2 的 MAC 地址后, 直接封装 webserver2 的 MAC 地址和 IP 地址。通过上面的分析, 可以得出正确答案是 C 和 E。用排除法也可以得出正确答案, 因为这里的处理过程与路由器 R1 无关, 排除提到路由器 R1 的 A、B、D 选项, 也可得出正确答案。

43. 解: D

题目问: 一个接收主机计算帧的校验和, 发现帧被破坏了, 这个帧被丢弃, 问这个过程是发生在 OSI 模型的哪一层? 提到帧, 大家就应该想到数据链路层, 在数据链路层封装帧头和帧尾, 其中的帧尾就是 CRC (循环冗余校验部分), CRC 就是用来检验帧的传送过程中有没有错误, 如果错误, 就丢弃帧。

44. 解：E

题目问：当排除网络连接故障问题时，一个工程师观察到工作站的网卡指示灯和工作站连接交换机的那个端口的指示灯都亮得很稳定，然而，当在工作站上执行 **ping** 命令时，输出的信息是 “Request timed out.”，问这个问题最可能出现在 OSI 模型的哪一层？既然工作站和交换机的指示灯都是亮着的，说明物理层没有问题，以太网上也不存在其他协议封装问题，数据链路层一般也不会有什么問題，造成 **ping** 不通的原因最可能发生在网络层，譬如 IP 地址配置错误码等问题。

45. 解：D

题目问：参照图，一个工程师排除网络连接的问题，这个主机不能 **ping** 通连接在交换机 A 上的服务器，基于测试结果，可能是什么问题？主机 **ping** 127.0.0.1 是成功的，说明 TCP/IP 协议栈已经成功安装，主机 **ping** 自己能够 **ping** 通，说明主机的网卡是正常的，从图中可以看出主机和路由器接口的 IP 地址配置正确，说明网络层的配置正确，以太网中的数据链路层一般没什么问题，主机 **ping** 不通本地网关，最可能的原因就是主机到路由器的连接有问题，是物理层的问题，**ping** 本地网关都不通，**ping** 远程主机不通是理所当然的，也得出远端物理层有问题。最可能的答案就是本地的物理层有问题。

第 3 章

以太网*

本章主要介绍以太网的发展、以太网中的关键字段、MAC（Media Access Control，介质访问控制）的功能和特点、以太网物理层和数据链路层的特点等。

3.1 以太网简介*

互联网工程任务组（Internet Engineering Task Force, IETF）维护 TCP/IP 协议上层的功能和服务，但是，OSI 模型的数据链路层和物理层的功能性和服务却有多个组织（IEEE、ANSI、ITU）描述，或由私有公司设计（专有协议）。以太网标准定义了第二层协议和第一层技术，虽然以太网支持不同的媒体、带宽，但所有以太网基本的帧格式和地址的架构是相同的。

1. IEEE 标准

在 1985 年，电气和电子工程师协会（Institute of Electrical and Electronics Engineers, IEEE）标准委员会为局域网和城域网制定了标准。这些标准以 802 开始，以太网的标准是 802.3。IEEE 希望其标准与国际标准组织（ISO）和 OSI 模型兼容，为了确保兼容性，IEEE 802.3 标准致力于 OSI 模型的第一层和第二层的较低部分。

如图 3-1-1 所示，以太网包括 OSI 模型的下二层，即物理层和数据链路层，而 IEEE 802.3 标准包括了 OSI 模型的物理层和数据链路层的下半部分（即 MAC 子层）。IEEE 802.2 规定了 OSI 模型数据链路层的上半部分（即 LLC 层，Logic Link Control，逻辑链路控制）。以太网包括了 IEEE 802.3 和 IEEE 802.2。

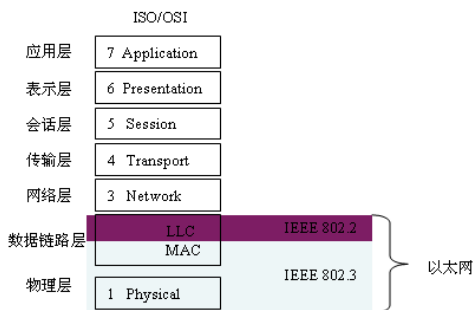


图 3-1-1 以太网和 IEEE 标准

2. 以太网的数据链路层

以太网把数据链路层的功能分成两个子层：LLC（Logical Link Control，逻辑链路控制）

和 MAC（Media Access Control，介质访问控制）。对以太网来说，IEEE 802.2 标准描述了 LLC 子层的功能，IEEE 802.3 标准描述了 MAC 子层和物理层的功能。

(1) **LLC 子层**。数据链路层使用 LLC 子层与上层协议进行通信。LLC 执行的是软件，它的执行与硬件设备独立。在计算机中，LLC 可以被认为是计算机的网卡驱动，网卡的驱动与网卡相互作用，在媒体和 MAC 子层之间传递数据。

LLC 子层的功能总结如下：

- 和上层协议进行通信；
- 把网络层的包转换成帧；
- 识别网络层的协议；
- 和物理层设备相对独立。

(2) **MAC 子层**。媒体访问控制（MAC）是以太网数据链路层下面的子层。媒体访问控制被硬件执行，典型的是计算机网络接口卡（Network Interface Card，NIC）。以太网 MAC 子层有两个主要任务：数据封装和媒体访问控制。

数据封装提供了 3 个主要职能：

- **帧的分界**：数据封装处理包括帧在传输之前的封装和在接收之后的解封装。MAC 子层在第 3 层 PDU 上增加头部和尾部形成帧，帧的处理提供了重要的分隔符号来识别组成帧的一组比特，帧和帧之间有分界符，用来同步发送端和接收端。
- **寻址**：封装还提供了数据链路层的寻址。在帧中增加的每个以太网头部包含物理地址（MAC 地址），使帧可以被送往一个目的地结点。
- **错误检测**：数据封装的一个额外功能是错误检测。每个以太网的帧的尾部包含帧内容的 CRC（Cyclic Redundancy Check，循环冗余校验）。收到一个帧后，接收结点计算一个 CRC，并与收到的 CRC 进行比较。如果这两个 CRC 匹配，表示收到的帧没有错误，可以信任。

媒体访问控制：MAC 子层控制把帧加载到传输介质上和从传输介质上卸载帧。顾名思义，它管理媒体的存取控制。这包括初始化的帧传输和从由于碰撞造成的传输失败中恢复。

逻辑拓扑：以太网的逻辑拓扑是一个多路访问总线，这意味着在该网络中的所有结点（设备）共享传输媒体。进一步意味着，在这个分段上的所有结点能接收到在这个分段上任何结点所传送的帧。因为所有结点能接收到所有的帧，每个结点需要判断是否需要接收和处理一个帧，这依赖于数据帧中的目的 MAC 地址。以太网提供了一个方法，确定结点如何共享访问媒体，媒体访问控制方法的经典是 CSMA/CD（Carrier Sense Multiple Access / Collision Detection，载波侦听多路访问/冲突检测），稍后的章节会介绍这种方法。

3. 以太网的发展

以太网起源于最初的 Alohanet，Alohanet 是一个数字无线网络，被设计用来在夏威夷群岛之间在一个共享的无线电频率上传输信息。Alohanet 要求所有的工作站对没有收到确认的数据包进行重传，这种使用共享媒体的技术后来被应用到今天以太网的有线技术中。第一代以太网使用的技术是 CSMA/CD。

早期以太网使用同轴电缆连接一个总线拓扑结构中的计算机，每一台计算机都直接连接到骨干。早期的以太网包括粗缆（thicknet，10base5）和细缆（thinnet，10base2）。10base5 允许的传输距离是 500m，10base2 允许传输的距离是 185m。早期部署的以太网，在低带宽

网络环境下,使用 CSMA 原理访问共享媒体,CSMA 后来发展成 CSMA/CD。使用同轴电缆的以太网在数据链路层是逻辑总线拓扑结构,在物理层也是总线拓扑结构。

后期 UTP 电缆取代了同轴电缆,UTP 电缆比较容易安装,重量轻,价格更便宜。使用集线器互连,物理拓扑改成星型拓扑。集线器相当于中枢,其他计算机通过 UTP 连接到集线器上,某台计算机电缆的故障不会影响整个网络。当某台计算机发送数据到达集线器时,集线器把数据转发到除接收端口以外的所有端口,在逻辑上仍是总线拓扑结构。因为媒体是共享的,在同一时间只能有一个工作站能成功传输,这种类型的连接被描述为半双工通信。随着以太网中设备的增加,发生碰撞的概率越来越大,通信的效率越来越低。

以太网的一个重大发展是交换机的出现,在以太网中使用交换机取代集线器。交换机为每一个工作站提供专用带宽,可以全双工工作,避免了冲突。交换机能够根据目的 MAC 地址对应的端口进行转发,无关的端口不受影响,这样就创建一个多路径的以太网网络,即多个无关的结点间可以同时发送数据,这种类型的通信被描述成全双工通信。

以太网交换机使用 5 个基本操作来完成功能:学习、老化、泛洪、选择性转发、过滤。

- **学习:** 交换机 MAC 地址表包含 MAC 地址和对应的端口。每一个帧进入交换机时,交换机审查源 MAC 地址,进行查找,如果 MAC 地址表中没包含这个 MAC 地址,交换机创建一个新的条目,包括源 MAC 地址和接收的端口。以后如果有去往这个 MAC 地址的帧,交换机则往对应的端口进行转发。
- **老化:** 交换机中的 MAC 地址条目有一个生存时间。每学到一个 MAC 地址条目,都附加一个时间值。随着时间的流逝,该数值一直减小,当数据值减小到 0 时,清除该 MAC 地址条目。如果有包含该 MAC 地址的新的帧到达,则刷新 MAC 地址的老化时间值。
- **泛洪:** 如果交换机收到一个数据帧,则可在交换机的 MAC 地址表中找,若找不到该数据帧的目的 MAC 地址,交换机转发该数据帧到除接收端口以外的所有端口,即广播该数据帧。如果交换机收到一个广播的数据帧,即数据帧的目的 MAC 地址是“FFFFFFFFFFFF”,交换机也会转发该数据帧到除接收端口外的所有端口。因为没有设备的 MAC 地址是“FFFFFFFFFFFF”,交换机根据数据帧的源 MAC 地址进行学习,永远也不会学到这个 MAC 地址。
- **选择性转发:** 交换机根据帧的目的 MAC 地址进行转发。当交换机收到某个数据帧时,交换机在 MAC 地址表中查找该数据帧的目的 MAC 地址,如果交换机已经学到这个 MAC 地址,数据帧将被转发到该 MAC 地址对应的端口,而不用泛洪到所有的端口。
- **过滤:** 在某些情况下,帧不会被转发,这个过程被称为帧过滤。一种情况是,交换机不转发帧到接收到的端口;另一种情况是,如果一个帧的 CRC 校验失败,帧也会被丢弃。使用帧过滤的另一个原因是安全方面的考虑,可以阻止或允许交换机转发特定的 MAC 地址到特定的端口。

以太网取得如此大的成功,有以下几个方面的因素:

- 简单和易于维护;
- 很容易合并新技术;
- 可靠性提高;
- 安装和升级的花费低。

4. CSMA/CD 工作原理

CSMA/CD 是英文 Carrier Sense Multiple Access/Collision Detection 的缩写，翻译成“载波侦听多路访问/冲突检测”或“带有冲突检测的载波侦听多路访问”。CSMA/CD 是一种争用型的介质访问控制协议。它起源于美国夏威夷大学开发的 ALOHA 网所采用的争用型协议，并进行了改进，使之具有比 ALOHA 协议更高的介质利用率。CSMA/CD 是一种分布式介质访问控制协议，网中的各个站（结点）都能独立地决定数据帧的发送与接收。所谓载波侦听（Carrier Sense），意思是网络上各个工作站在发送数据前都侦听总线上有没有数据传输。若有数据传输（称总线忙），则不发送数据；若无数据传输（称总线空），则立即发送准备好的数据。所谓多路访问（Multiple Access），意思是网络上所有工作站收发数据共同使用同一条总线，且发送数据是广播式的。所谓冲突（Collision），意思是若网上有两个或两个以上工作站同时发送数据，在总线上就会发生信号的碰撞，造成信号的混合，哪个工作站都辨别不出真正的数据是什么。为了避免数据在发送过程中产生冲突，工作站在发送数据过程中还要不停地检测自己发送的数据，有没有在传输过程中与其他工作站的数据发生冲突，这就是冲突检测（Collision Detection）。CSMA/CD 媒体访问控制方法的工作原理可以概括如下：

- 先听后说，边听边说；
- 一旦冲突，立即停说；
- 等待时机，然后再说；
- 听，即监听、检测之意；
- 说，即发送数据之意。

在发送数据前，先监听总线是否空闲。若总线忙，则不发送；若总线空闲，则把准备好的数据发送到总线上。在发送数据的过程中，工作站边发送边检测总线，看是否自己发送的数据有冲突。若无冲突，则继续发送直到全部数据传完为止；若有冲突，则立即停止发送数据，但是要发送一个加强冲突信号，以便使网络上所有工作站都知道网上发生了冲突，然后，等待一个预定的随机时间，且在总线为空闲时，再重新发送未发完的数据。



3.2 以太网帧*

在第 3 层的 PDU 上添加头部和尾部形成帧，以太网头部和尾部的几个部分被以太网协议使用，帧的每一部分叫做域。有两种类型的以太网帧：原始的 IEEE 802.3 和修订后的 IEEE 802.3（也就是以太网）。这两种类型之间的差异微乎其微，它们之间最明显的差异是，原始的 IEEE 802.3 多了一个 SFD（Start Frame Delimiter，起始帧分界符）和类型域中包括了长度这一小的改变，如图 3-2-1 所示，图中第一行表示的是字节数，第二行表示的是字段域。

802.3 的帧

7	1	6	6	2	46~1500	4
Preamble(前 导位)	Start of Frame delimiter(起始 帧分界)	Destination Address(目的 MAC 地址)	Source Address(源 MAC 地址)	Length/Type (长度/类型)	802.2 Header and Data(802.2 头 部和数据)	Frame Check Sequence(帧 检验序列)

以太网的帧

8	6	6	2	46~1500	4
Preamble (前导位)	Destination Address (目的 MAC 地址)	Source Address (源 MAC 地址)	Length/Type (长度/类型)	802.2 Header and Data (802.2 头部和数据)	Frame Check Sequence (帧校验序列)

图 3-2-1 两种帧格式

1. 以太网帧大小

最初的以太网标准定义了帧最小为 64 个字节,最大为 1518 个字节。这包括从目的 MAC 地址域到帧校验序列域之间的所有字节,前导位和起始帧分界域不包括在内,从图 3-2-1 中也可以计算出来。1998 年发布的 IEEE 802.3ac 标准中,延长了所允许的最大帧大小到 1522 个字节。帧中增加的 4 个字节用来容纳一个新技术——虚拟局域网 (VLAN),有关 VLAN 的知识将在交换机部分介绍。

如果帧小于 64 个字节或大于 1522 个字节,被认为是非法的帧,非法的帧将被丢弃。

2. 以太网 MAC 地址

MAC 地址用来确保以太网设备的全球唯一性。IEEE 要求任何生产以太网设备的厂商进行登记,并分配一个 3 个字节的厂商代码,叫做组织唯一标识符 (Organizationally Unique Identifier, OUI)。

IEEE 要求供应商遵循两个简单的规则:所有分配给网卡或其他以太网设备的 MAC 地址必须使用供应商分配的 OUI 为前 3 个字节;后 3 个字节是每个厂商生产的唯一设备编号。MAC 地址一般在生产时被烧入 ROM (Read-Only Memory, 只读存储器),这意味着,MAC 地址不能被改变,但可以改变 MAC 地址的显示,当计算机启动时,网卡拷贝地址信息到内存中,用来判断接收的数据帧是否是发往本机的,可以通过软件和网卡自动的驱动来改变 MAC 地址的显示。

当网络设备转发数据时,目的 MAC 地址信息被添加到帧头中,源设备发送数据到网络上,网络上所有接收到这个数据的设备都查看数据帧中的目的 MAC 地址是否与本机的相同,如果相同,则进行解封装并上传给上层;如果不相同,则丢弃该数据帧。

不同的硬件和软件制造商表示 MAC 地址的形式不一定相同,大概有下面 3 种表示格式:00-11-bc-35-ab-40、0011.bc35.ab40 和 00:11:bc:35:ab:40。

3. 单播、组播和广播

在以太网中,第二层使用不同的 MAC 地址:单播、广播和组播,如图 3-2-2 所示。

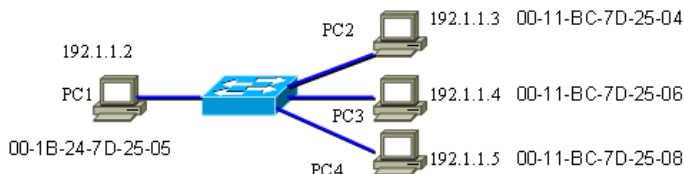


图 3-2-2 单播、广播和组播帧

(1) 单播帧

当单一源设备发送数据帧给单一目的的设备时，单播 MAC 地址被使用。在图 3-2-2 中，PC1 给 PC2 发送数据，帧的内容如图 3-2-3 所示，是一个单播帧。

目的MAC	源MAC	目的IP	源IP	数据	帧尾
00-11-BE-7D-25-04	00-1B-24-7D-25-05	192.1.1.3	192.1.1.2	数据	FCS

图 3-2-3 单播帧

(2) 广播帧

当单一源设备发送数据给同一个网段上的所有设备时，目的 MAC 地址是“FF-FF-FF-FF-FF-FF”，这是一个广播帧。在图 3-2-2 中，假如 PC1 发送一个子网广播，帧的内容如图 3-2-4 所示，是一个广播帧。

目的MAC	源MAC	目的IP	源IP	数据	帧尾
FF-FF-FF-FF-FF-FF	00-1B-24-7D-25-05	192.1.1.255	192.1.1.2	数据	FCS

图 3-2-4 广播帧

(3) 组播帧

当单一源设备发送数据给同一组设备时，目的 IP 地址是一个组播 IP 地址，目的 MAC 地址是以“01-00-5e”打头的，组播 IP 地址和组播 MAC 地址之间有一种对应关系，CCNP 中会介绍到这一点。在图 3-2-2 中，假如 PC1 运行了 RIPv2，PC1 发送 RIPv2 的路由信息到组播 IP 地址 224.0.0.9，帧的内容如图 3-2-5 所示，是一个组播帧。

目的MAC	源MAC	目的IP	源IP	数据	帧尾
01-00-5E-00-00-09	00-1B-24-7D-25-05	224.0.0.9	192.1.1.2	数据	FCS

图 3-2-5 组播帧

4. 双工模式

以太网上有两种双工模式：半双工（Half-duplex）和全双工（Full Duplex）。

(1) 半双工

半双工通信只能是单向数据流，并不在同一时刻同时发送和接收数据。这类似于对讲机，说话的时候就不能听，听的时候就不能说话，听和说不能同时进行。如果有两个设备同时发送数据，就发生了碰撞。因此，半双工通信采用的是 CSMA/CD，以帮助减少潜在的碰撞和碰撞后处理。半双工通信的数据流在一个时刻只能在一个方向上传输，因此性能较差。半双工连接通常是在较旧的硬件设备上，如集线器（Hub），如图 3-2-6 所示。

(2) 全双工

全双工通信中数据流是双向的，在同一时刻可以同时发送和接收数据。双向传输可以提高性能，减少传输的等待时间。现在的以太网、快速以太网、千兆位以太网网卡都支持全双工。交换机也支持全双工。在线缆两端连接的设备都支持全双工的情况下，线路的冲突检测功能被禁用。线路可以用同样的速度同时进行发送和接收，吞吐量可以达到链路带宽的两倍。在图 3-2-7 中的设备都可以工作在全双工模式下。

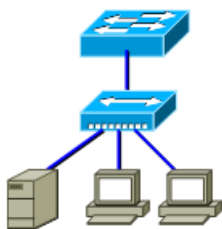


图 3-2-6 半双工模式

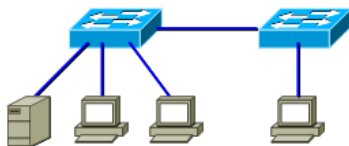


图 3-2-7 全双工模式



3.3 真题精选*

1. Which statement is true about full-duplex Ethernet in comparison to half-duplex Ethernet?

- A. Full-duplex Ethernet consists of a shared cable segment. Half-duplex Ethernet provides a point-to-point link.
- B. Full-duplex Ethernet uses a loopback circuit to detect collisions. Half-duplex Ethernet uses a jam signal.
- C. Full-duplex Ethernet can provide higher throughput than can half-duplex Ethernet of the same bandwidth.
- D. Full-duplex Ethernet uses two wires to send and receive. Half-duplex Ethernet uses one wire to send and receive.

2. A network interface port has collision detection and carrier sensing enabled on a shared twisted pair network. From this statement, what is known about the network interface port?

- A. This is a 10 Mb/s switch port.
- B. This is a 100 Mb/s switch port.
- C. This is an Ethernet port operating at half duplex.
- D. This is an Ethernet port operating at full duplex.
- E. This is a port on a network interface card in a PC.



3.4 真题解答*

1. 解: C

题目问: 全双工以太网与半双工以太网相比, 哪个语句描述是正确的? 全双工和半双工的区别: 全双工是同时既能收也能发, 而半双工是在收的时候不能发, 发的时候不能收。所以全双工可以更有效地利用带宽, 对于相同的带宽, 全双工比半双工能提供更高的吞吐量。A 选项说全双工以太网是共享链路, 半双工以太网是点对点链路, 这种说法恰恰相反; B 选项说全双工以太网使用回环电路检测冲突, 半双工以太网使用 jam (阻塞) 信号。全双工中不存在冲突, 半双工通过发送 jam 信号, 来让所有设备知道发生了冲突; C 选项说在同样的带宽上, 全双工以太网可以比半双工以太网提供更高的吞吐量, 该选项正确; D 选项说全双工使用两根线来发送和接收, 半双工使用一根线来发送和接收。半双工使用一对电

缆线，而不是一根，数字信号在线路上是双向传输的。全双工以太网使用两对（不是两根）电缆线，在发送设备的发送方和接收方之间采用点到点连接。

2. 解：C

题目问：一个网络接口在共享的双绞线网络中有冲突检测和载波侦听的功能，可以得知这个网络接口是什么接口？一个接口有冲突检测和载波侦听，而且是使用双绞线的网络，那么可以推测出这个接口是以太网接口，而且工作在半双工模式下。

第 4 章

思科路由器**

本章介绍路由器的硬件和软件，主要内容有：思科 Packet Tracer 模拟器的使用、用“Dynamips”搭建 CCNA 实验台、路由器基本硬件、基本软件、路由器的引导过程、思科的命令行接口介绍、路由器的基本配置、CDP 协议的使用等。



4.1 模拟设备的使用

中国有句古话，叫“巧妇难为无米之炊”，学习网络更是这样，没有路由器和交换机，最终只能是纸上谈兵。然而 Cisco 的路由器和交换机价格昂贵，动辄几千元，甚至几十万元，远远超出了个人的购买能力。若想配置路由器和交换机，除了参加社会培训外，几乎别无选择。即使参加社会培训，时间也是短暂的，设备更是有限，难以满足需求。如何解决这一棘手难题？这里很荣幸地向大家推荐两款经典的模拟软件“Packet Tracer”和“Dynamips”。

4.1.1 Packet Tracer 模拟器的使用

Cisco 公司针对其 CCNA 认证专门开发了一个用来设计、配置和故障排除的官方模拟软件 Packet Tracer。使用者可以自己选择设备，包括路由器、交换机、集线器、无线 AP、无线宽带路由器、各种线缆、计算机和服务器等，然后完成设备的配置，并能进行测试，感觉和真实场景几乎没有差别。

Packet Tracer 是网络入门的经典模拟器，适合新手学习 CCNA 使用，具有真实的操作界面，很容易上手，几乎支持 CCNA 涉及的所有内容，目前的最新版本是 5.2.1。这个模拟器比其他任何第三方的模拟器（比如 BOSON）更加人性化，更加有身临其境的感觉，对 CCNA 支持得更强。但是，它只支持 CCNA 中的一些内容，对初学者有很大的帮助，不支持 CCNP、CCIE 部分的复杂实验。下面演示 Packet Tracer 的安装和使用。

1. 安装 Packet Tracer

从<http://blcui.njut.edu.cn/CCNANEW.rar>下载软件包，解压缩到硬盘，然后双击软件包中的“PacketTracer5.2.1 中文版\PacketTracer521_setup.exe”文件，完成 Packet Tracer 的安装。

2. Packet Tracer 主界面介绍

双击桌面上的“Cisco Packet Tracer”快捷图标，运行 Packet Tracer，打开 Packet Tracer 主界面，如图 4-1-1 所示。主界面中提供了很多选项，但很多选项在工程中用不到，考试中也并不会涉及，本书仅仅介绍可以用到的功能，更多的功能选项可以查看 Packet Tracer 的联机帮助。

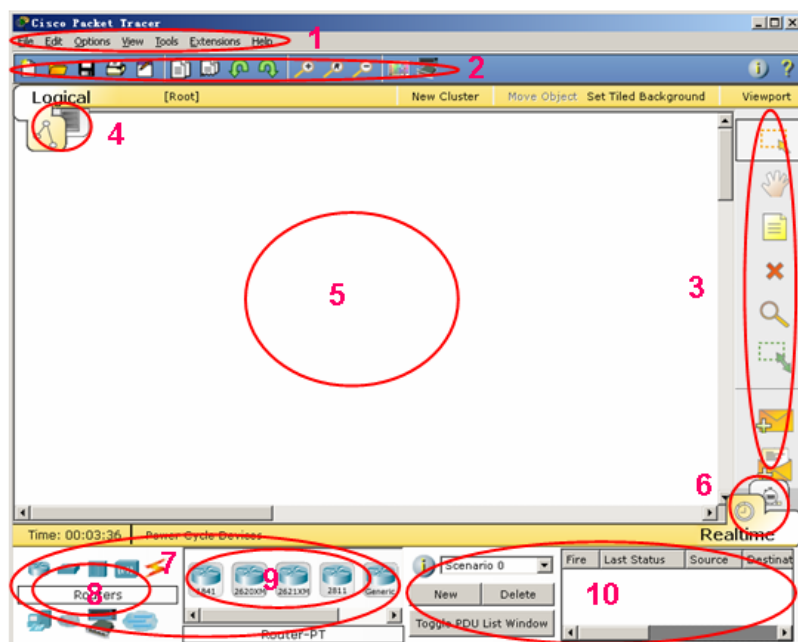


图 4-1-1 Packet Tracer 主界面

在图 4-1-1 中：

- 区域 1 是菜单项，包括文件、编辑、选项、查看、工具、扩充、帮助菜单。各菜单又包括相应的子菜单。
- 区域 2 是快捷工具栏，能用到的有：新建、打开、保存、打印、复制、粘贴、撤销、放大、还原、缩小等快捷图标。
- 区域 3 是一般工具栏，能用到的有：选中、注释、移动设备、删除设备等按钮。
- 区域 4 是逻辑和物理切换按钮，物理就是设备的实际物理分布图。读者只需要使用逻辑拓扑就可以了，不用理会物理拓扑。
- 区域 5 是工作区域，在此可以创建拓扑。从区域 9 中选择设备和线缆拖入区域 5 并连接，搭建逻辑拓扑图。
- 区域 6 是实时和模拟场景。实时场景相当于是工作状态，模拟场景相当于是教学模式，在模拟场景下可以捕获特定的协议，并分析协议包中的内容。模拟场景下设备的运行速度较慢，正常做实验时，要切换到实时场景。
- 区域 7 是设备选择窗口。
- 区域 8 是设备类型选择窗口，包括路由器、交换机、集线器、无线设备、线缆、计算机、网云、用户自定义设备。
- 区域 9 是某种类型设备具体的设备型号，比如在区域 8 中选择路由器，区域 9 中会列出模拟器可以支持的所有路由器型号，然后从区域 9 中选择某款路由器，并把路由器拖入到工作区域 5 中。
- 区域 10 是工作在模拟场景下，管理包的窗口，一般情况下也用不到，这里不用理会。

3. 汉化

Packet Tracer 是一款很好的 Cisco 模拟器，如果英语不好用起来不是很方便，这里介绍

汉化的方法。把软件包的“PacketTracer5.2.1 中文版\chinese.ptl”文件复制到安装目录的languages 文件夹下，默认的位置在“C:\Program Files\Packet Tracer 5.2\languages”。单击 Packet Tracer 主界面中的菜单“Options”→“Preferences”，打开“Options”对话框，在“Select Language”列表框中选择“Chinese.ptl”，然后单击“Change Language”按钮，提示重启 Packet Tracer 后，汉化将起作用。关闭 Packet Tracer，再次运行，汉化成功。

4. 搭建逻辑拓扑

(1) 添加设备


在 Packet Tracer 中创建如图 4-1-2 所示的逻辑拓扑图。在图 4-1-1 的区域 8 中选择路由器，然后从区域 9 中选择第一台思科 1841 路由器，如图 4-1-3 所示。



图 4-1-2 逻辑拓扑图

图 4-1-3 选择具体型号的路由器

把该路由器拖入图 4-1-1 的区域 5 中，并把鼠标停留在该路由器上，会出现一个弹出窗口，显示该路由器有哪些接口，以及每个接口的状态，如图 4-1-4 所示。后面的课程中会介绍到一个命令，可以在路由器上查到类似的信息。



1841 Router

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/0	Down	--	<not set>	000A.41B9.8D01
FastEthernet0/1	Down	--	<not set>	000A.41B9.8D02
Vlan1	Down	1	<not set>	0002.1625.CA60

Hostname: Router

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

图 4-1-4 路由器接口及状态提示

(2) 添加模块

从图 4-1-4 中可以看到路由器有两个快速以太网口，可并没有串行接口（Serial 口，串行接口一般用于广域网的连接），满足不了图 4-1-2 中的要求。这就相当于用户在买设备，设备默认配置不满足，那就再加选配件，只不过现实中需要花银子，这里只要点选一下就可以了。

单击图 4-1-4 中的路由器，打开如图 4-1-5 所示的窗口。窗口中的区域 1 是思科 1841 可以支持的模块类型，区域 2 是具体模块的说明，区域 3 是具体模块的外观，区域 4 和区域 5 是路由器上没有使用的扩展槽，区域 6 标出的是路由器的电源开关。这和平时添加计算机的配置差不多，比如要添加的是声卡、网卡、显卡或内存，要考虑计算机上有没有可用的插槽。当然在添加模块时，要关闭路由器的电源，就像在计算机中添加一块网卡，也要断开计算机的电源，要知道带电操作不仅会损坏设备，也会给人带来生命危险。如果没有关闭电源，从区域 1 中拖动模块到区域 4 或区域 5，Packet Tracer 会提示“Cannot add a modult when the power is on”，Packet Tracer 真不愧是思科官方的模拟器，设计得如此强大和人性化，实在令人佩服。

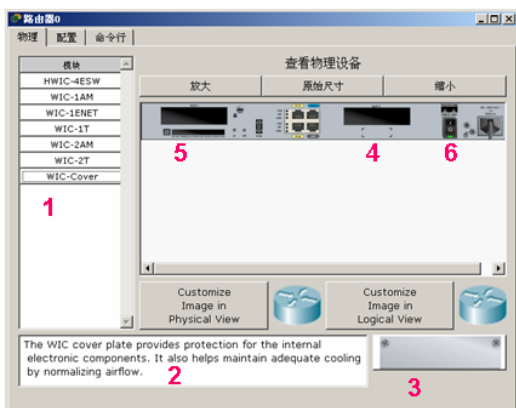


图 4-1-5 设备配置窗口

单击区域 6 中标出的路由器电源，区域 6 中的绿灯灭掉，表示断开了电源。单击区域 1 中的 WIC-1T，选择有一个 Serial（串行）接口的模块，或者单击 WIC-2T，选择有两个串行接口的模块。从区域 3 中可以看到 WIC-1T 模块是大口的串行模块，WIC-2T 模块是小口的串行模块，请在两台路由器上选择同一型号的串行模块，本书中都使用 WIC-2T 模块。拖住 WIC-2T 模块到区域 4 的空槽上，不能拖到区域 5 的空槽上，因为图 4-1-2 中标明了是 S0/0/0 接口，如果把 WIC-2T 模块拖到区域 5 上，路由器的两个串口编号是 S0/1/0 和 S0/1/1。添加完模块后，单击路由器的电源开关，给路由器加电。

图 4-1-5 中的“配置”标签是图形化的配置命令，对学习没有帮助，不推荐使用，“命令行”（CLI，Command Line Interface 命令行接口）标签是读者经常要用到的命令行接口，本书涉及的多数配置都是在命令行窗口中完成的，稍后会介绍命令行接口。

（3）添加自定义设备

如果经常要使用有两个串行接口的 1841 路由器，每次都添加模块太烦琐。这里可以把上面配置好的路由器加入自定义设备中，以后就可以直接调用了。

单击图 4-1-1 的区域 2 中的最后一个图标“Custom Devices Dialog”，打开设备模板管理窗口，如图 4-1-6 所示。

单击图 4-1-6 中的“Select”按钮，对话框消失，单击刚才在工作区域添加的 1841 路由器，出现如图 4-1-7 所示的窗口。给自定义的 1841 路由器起一个直观的名字“1841-2F-2S”，在描述中随便输入“1841 with 2Fa + 2S”，单击“Add”按钮，出现保存文件对话框，给自己创建的设备随便起一个文件名保存。单击图 4-1-1 的区域 8 中的“Custom Made Devices”类，可以在右边的分类中看到自己创建的设备 1841-2F-2S，直接拖入工作区域就可以了。

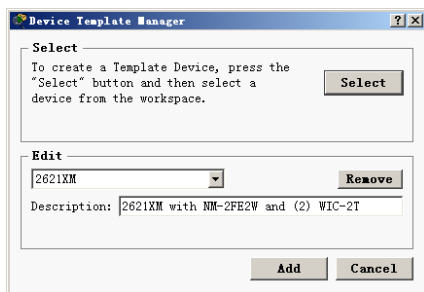


图 4-1-6 在设备模板管理窗口选择设备

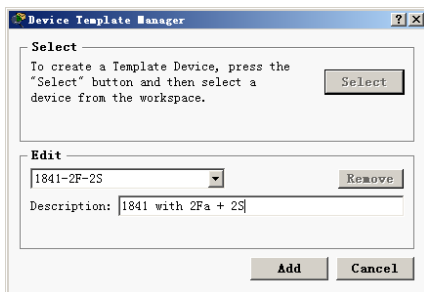


图 4-1-7 在设备模板管理窗口添加设备

(4) 继续添加其他设备

使用上面的方法继续添加思科交换机 2960、PC 和服务器的画面如图 4-1-8 所示。

(5) 添加连线

添加完网络设备后, 接下来添加它们之间的连线, 单击图 4-1-1 的区域 8 中的“线缆”, 在图 4-1-1 的区域 9 中显示可用的连接线缆, 如图 4-1-9 所示。

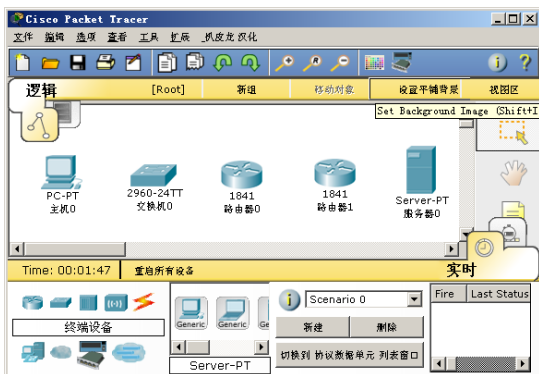


图 4-1-8 添加完网络设备的画面



图 4-1-9 线缆类型

图 4-1-9 中的第一种线缆是自动线缆(根据场合自动选择线缆类型, 不建议读者使用这种线缆); 第二种线缆是“配置线”, 英文的意思是 Console, 是连接计算机 COM 口和路由器或交换机 Console 口的线缆; 第三种线缆是“直通线”, 英文的意思是 Copper straight-through, 直通双绞线; 第四种线缆是“交叉线”, 英文的意思是 Copper Cross-over; 第五种线缆是“光纤”, 英文的意思是 Fiber; 第六种线缆是“电话线”, 英文的意思是 Phone; 第七种线缆是“同轴电缆”, 英文的意思是 Coaxial; 第八种线缆是“DCE 串口”, 英文的意思是 Serial DCE, 用于连接串行接口, 一根串行线连接两台设备, 线缆的一端标明 DCE, 另一端标明 DTE, 需要在 DCE 端配置时间钟来保持同步, 这种线缆的起始端是 DCE, 终止端是 DTE; 第九种线缆是“DTE 串口”, 与第八种线缆相似, 只不过起始端是 DTE, 终止端是 DCE。

图 4-1-8 中的 PC 和 2960 交换机之间应该使用的是直通双绞线, 也就是选择第三种线缆。用鼠标单击第三种线缆, 把鼠标移到工作区域, 可以发现鼠标的指针变成线缆的形状, 用鼠标单击 PC, 提示选择接口类型, 如图 4-1-10 所示。



图 4-1-10 选择接口

选择 FastEthernet (快速以太网) 接口, 即 PC 的网卡。然后拖动线缆另一端到 2960 交换机上并单击, 提示选择 2960 的接口, 根据图 4-1-2 中的要求, 选择 FastEthernet 0/2 接口。继续选择直通双绞线连接 2960 和 Router0 的 FastEthernet 0/1 接口。选择交叉双绞线连接路由器 Router0 和 Router1 的 FastEthernet 0/0 接口。选择第八种交叉线缆连接 Router0 和 Router1 的 Serial 0/0/0 接口, Router0 端是 DCE, Router1 端是 DTE。选择交叉双绞线连接 Router1

的 FastEthernet 0/1 接口和 Server0 的快速以太网接口。连接完成后的拓扑图如图 4-1-11 所示。

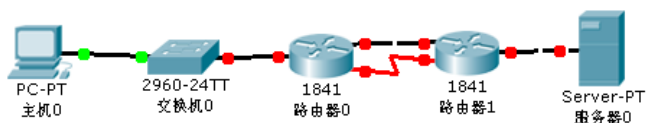


图 4-1-11 Packet Tracer 中的拓扑图

如果读者连错线或选错了设备，可以单击图 4-1-1 的区域 3 中的“Delete”图标，然后再单击对应的设备或线缆即可删除。读者会注意到 PC 和 2960 交换机之间的线缆有绿色标记，这表示线缆是通的；除此之外的线缆都有红色标记，这表示线缆是不通的。至于为何出现这种情况，本书后面会介绍。

在图 4-1-11 中看不到线缆连接设备的端口，将鼠标移到线缆上，线缆两端自动显示连接设备的端口号。如果想要端口一直显示，可以单击菜单“选项”→“首选项”，打开如图 4-1-12 所示的对话框，选中“显示端口标签”复选框。用户可以自定义，譬如选择关闭动画和声音、隐藏设备标签、显示端口标签等。

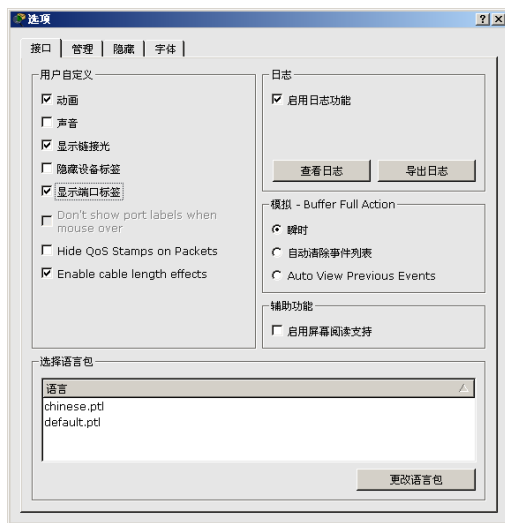


图 4-1-12 选择显示端口标签复选框

显示端口标签和隐藏设备标签后的拓扑图如图 4-1-13 所示。如果读者不习惯这种界面，可以取消显示端口标签选项。

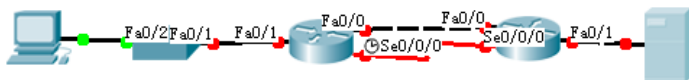


图 4-1-13 显示端口标签的拓扑图

至此，完成了 Packet Tracer 软件的安装和拓扑的设计。把这样的拓扑保存起来，以后使用时，直接打开拓扑即可。单击“保存”图标，打开如图 4-1-14 所示的保存对话框。

起一个文件名进行保存。

光盘中的第 2 章视频部分介绍了 Packet Tracer 模拟场景的使用，Packet Tracer 用在教学上，简直是无与伦比。

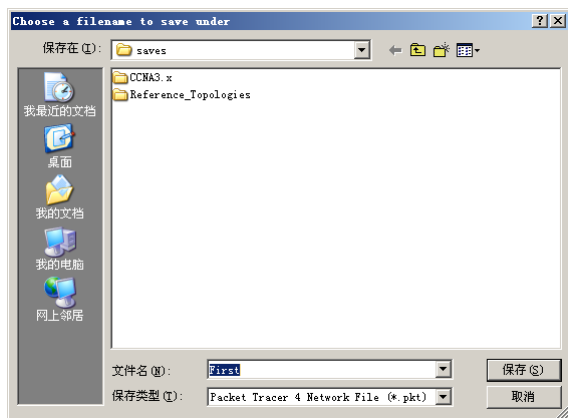


图 4-1-14 保存对话框

4.1.2 用“Dynamips”搭建 CCNA 实验台

Packet Tracer 虽好，但它毕竟是一款基于软件的模拟器，无法用于真实的环境，也无法完成高级的实验。这里介绍另外一款经典的路由器和交换机的模拟软件 Dynamips，在此，非常感谢 Dynamips 的作者“Chris”，是他的辛勤耕耘，使我们有这样一个方便学习的机会。虽然以往也有很多款 Cisco 路由器和交换机的模拟软件，但是任何一款路由器和交换机的模拟软件都不能与 Dynamips 相提并论，因为它与以往的模拟软件有本质上的区别。首先，Dynamips 模拟的是路由器和交换机的硬件，至于加载什么版本的 IOS（Internet Operate System，路由器或交换机的操作系统，相当于计算机是安装 Windows XP，还是安装 Windows Server 2003 等），完全由用户决定，而以往的模拟软件都是同时模拟硬件和软件，功能受限不谈，往往更是 Bug 连连，Dynamips 模拟的路由器具有真实路由器的所有功能；其次，Dynamips 模拟出的路由器和交换机可以与真实的网络互连，甚至可以用于实际的生产环境，而以往的模拟器却只是一个虚拟环境，无法与真实的网络相连。

既然 Dynamips 这么优秀，为何前面还要介绍 Packet Tracer 模拟器，这是因为 Dynamips 只能模拟路由器，虽然可以在路由器上安装交换模块来模拟交换机，但配置命令与现在多数纯交换机的配置命令有细微的差异，为了不影响大家参加 CCNA 考试，本书中很多涉及交换的实验大多在 Packet Tracer 模拟器中完成。为了拉近读者与真实环境的距离，培养大家更多的工程经验，多数配置和实验尽可能在 Dynamips 中完成，不能在 Dynamips 中完成的，才考虑在 Packet Tracer 模拟器中完成。

1. 实验台拓扑

为了便于大家完成本书相关的路由和交换实验，笔者给大家搭建了如图 4-1-15 所示的网络拓扑，拓扑中包括 6 台 Cisco3640 路由器，其中 3 台路由器配置了一个 16 口的交换模块，充当交换机 SW1、SW2、SW3，另外 3 台路由器 R1、R3 和 R4 配置了 2 个快速以太网模块；1 台 Cisco7200 路由器，也配置了 2 个快速以太网模块，主要用于完成一些复杂配置；R1、R2、R3 和 R4 都配置了一块 4 个串行端口的广域网模块；SW4 是不可配置交换机，4 个端口分别接 R1、R2 和 R3 的 4 个快速以太网接口，还有 1 个端口连接“真实计算机”的物理网卡；从图中可以看出“真实计算机”、因特网等都接到了这个实验环境中；4 台 Cisco3620 的路由器，用来模拟 PC。

2. 安装 “Dynamips”

为了能愉快地完成本书中的大部分实验，计算机的配置越高越好，推荐最低配置为：

- CPU 1500MHz，最好是 3000MHz 以上，双核的更好
- 内存 512MB，最好是 1GB，2GB 更好
- 空闲硬盘空间 2GB 以上
- 操作系统 Windows XP/Windows Server 2003

按如下步骤操作，进行初始化安装，以后就可直接使用实验台中的设备了。

- ① 把 CCNANEW.rar 中的文件 “CCNA dynamips.rar” 解压缩到任何位置。
- ② 进入 setup 子目录对模拟器进行整体参数的配置。
- ③ 双击 “1.安装 Win_Pcap”，根据屏幕提示，完成 Win_Pcap 的安装。
- ④ 双击 “2.获取网卡参数”，打开如图 4-1-16 所示的窗口，选中图中所示部分 “\Device\NPF_{D9D333A4-CF15-4A3D-BC07-9DF5F0DD0872}”，这里一定不要选错，按回车键进行复制。

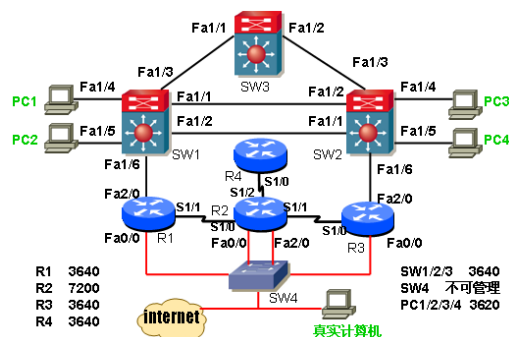


图 4-1-15 CCNA 机架网络拓扑



图 4-1-16 获取网卡参数

⑤ 用记事本打开 “labini\ccna.net” 文件，用图 4-1-16 中选中的部分替换图 4-1-17 中选中的部分，把这个网卡参数换成读者真实的网卡参数，保存修改后的配置文件。

⑥ 返回到 CCNA dynamips 目录。

⑦ 双击 “0.启动虚拟服务” 打开控制台，会出现如图 4-1-18 所示的窗口。实验结束前，不能关闭该窗口。

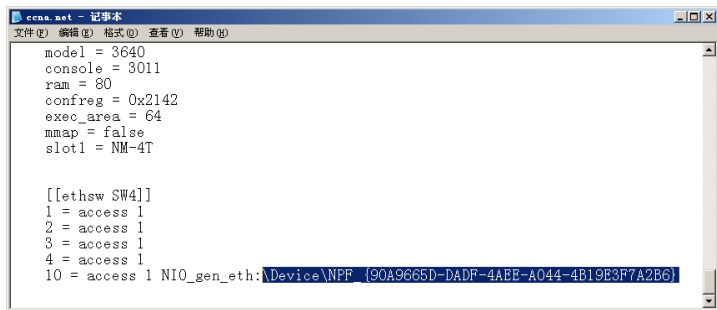


图 4-1-17 修改网卡参数

⑧ 双击 “1.控制台 CCNA.cmd” 会出现如图 4-1-19 所示的窗口。该窗口相当于所有设备的管理控制台，实验结束前，也不能关闭该窗口。



图 4-1-18 Dynamips 虚拟服务窗口

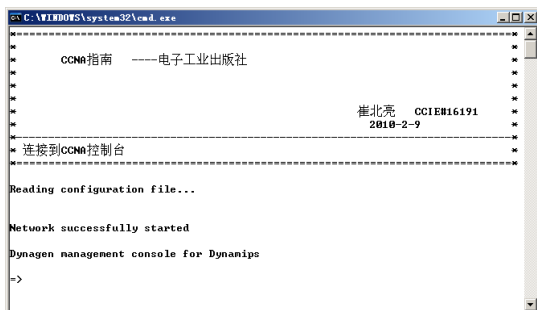


图 4-1-19 CCNA 机架控制台窗口

使用 list 命令查看设备列表, 如图 4-1-20 所示, 可以看到有 4 台交换机、4 台 PC、3 台路由器, 所有设备都处在停止状态, 其中 SW4 是不可管理交换机。然后使用命令 start R1 来启动路由器 R1, 注意这里是区分大小写的。这时会出现如图 4-1-20 所示的警告信息, 系统提示路由器 R1 没有配置 idle-pc 值。路由器在没有配置 idle-pc 值的情况下, 也可以运行, 只是 CPU 利用率会过高。大家此时可以查看一下计算机的 CPU 利用率, 一般都会在 50% 以上。

使用命令 idlepc get R1 来获得 idle-pc 值, 稍后会出现如图 4-1-21 所示的画面。

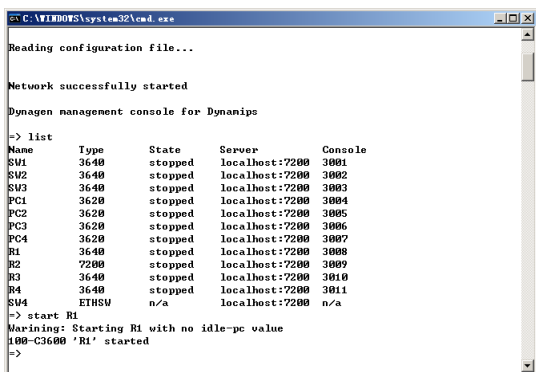


图 4-1-20 开启一台路由器

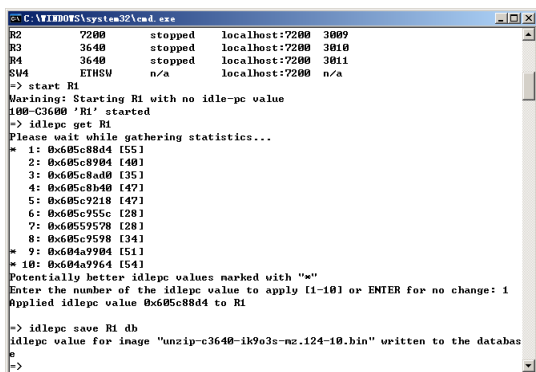


图 4-1-21 获取 idle-pc 值

带*号的 idle-pc 值为系统推荐的最佳值, 键入最佳选项前面对应的 1 到 10 的编号, 如果没有最佳推荐值, 就选择 “[]” 括号中值最大的那个选项, 回车后返回提示符状态。此时可以再次查看计算机的 CPU 利用率, 一般都会降到 10% 以下。

为了避免每次启动路由器都需要调整 idle-pc 值, 可以使用命令 idlepc save R1 db, 把路由器 R1 的 idle-pc 值保存起来, 如图 4-1-21 所示。可以打开“dynamips\workingdir\idlepcdb.ini”文件, 如图 4-1-22 所示, 该文件会记录下 IOS 文件名和对应的 idle-pc 值, 以后再运行使用同样 IOS 文件的路由器时, 自动使用此 idle-pc 值。也就是说, 对于很多个使用同一个 IOS 文件的路由器, idle-pc 值只需要获取一次。

3. “Dynamips” 的使用方法

- 使用 “?” 可以查看所有可用的命令。注意设备名和命令是区分大小写的。
- 使用 “list” 命令可以查看设备列表。
- 使用 “start” 命令可以打开路由器, 例如使用 “start R1” 开启 R1, 使用 “start /all” 开启所有设备。

- 使用“stop”命令可以关闭路由器，例如使用“stop R1”停止 R1，使用“stop /all”停止所有设备。
- 使用“reload”命令可以重启路由器，例如“reload R1”、“reload /all”。该命令相当于先停止一台设备，然后再开启这台设备，也可以使用 stop 和 start 组合来代替。
- 使用“telnet”命令可以登录到路由器的 console 接口，例如使用“telnet R1”，将打开 R1 的控制台。

在如图 4-1-21 所示的窗口中输入“telnet R1”后回车，弹出如图 4-1-23 所示的窗口；也可以单击“开始”→“运行”，输入“telnet localhost 3008”或“telnet 本机 IP 地址 3008”后回车，即可登录到 R1 的控制台，其中，3008 是图 4-1-20 中 R1 后面所对应的 Console（控制口）值。类似地，如果登录 SW1，则要把 3008 改成 3001；也可以在远程计算机上“telnet 运行模拟器的计算机的 IP 3008”登录到 R1 的控制台。如果是 R2，只要把端口从 3008 改成 3009，其他设备依此类推。为便于编辑，也可在“SecureCRT”软件中使用 Telnet 的方式打开路由器的控制台。CCNANEW.rar 中提供了 SecureCRT 软件。

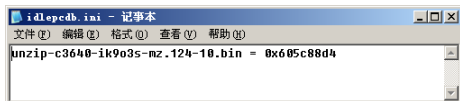


图 4-1-22 idlepcdb.ini 文件

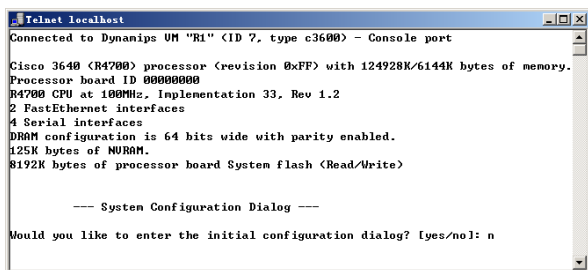


图 4-1-23 路由器 R1 的控制台

全部实验完成后，只要关闭如图 4-1-18 所示的服务窗口和如图 4-1-19 所示的控制台窗口就可以了。下次做实验的步骤与第一次实验差不多，依次打开服务窗口，打开控制台窗口，开启相关的设备，登录对应的设备，完成实验配置。

4. 设计“Dynamips”的拓扑

至此，我们完成了 CCNA 机架的搭建。到目前为止，“Dynamips”支持的硬件型号有 Cisco 7200、Cisco 3600（3620、3640、3660）、Cisco 2691、Cisco 3725、Cisco 3745，作者几乎每个星期都有更新。如果对这样的实验环境不满意，完全可以通过修改“dynamips\labini\ccna.net”文件来重新设计拓扑、修改设备型号、更换 IOS 版本等。为了大家可以自己构建拓扑，这里对 ccna.net 文件中的部分命令行解释如下，斜体部分为注释。

```
autostart = false    开启机架后，所有的设备都是停止状态，需要手工启动。如果把这里的 false 改成
                      true，则开启机架后，所有的设备都自动启动。

[localhost]          localhost 表示本机。
  port = 7200         dynamips 服务使用的端口是 7200，这里填的端口要和“0.启动虚拟服
                      务.bat”文件中调用的端口一致。
  workingdir = ..\workingdir\
                      dynamips 工作的目录为 dynamips\workingdir，运行中产生的临时文件、保存的配置、
                      idlepc.ini 文件等都保存在该目录下。该目录下的所有文件都可以删除，只是删除 idlepc.
                      ini 后，所有 IOS 的 idle-pc 值需重新获取，建议可以定期删除 idlepc.ini 以外的其他文件。

[[router SW1]]       第一台网络设备，名字叫 SW1。
  image = ..\IOS\unzip-c3640-ik9o3s-mz.124-10.bin
                      该路由交换机使用的 IOS 文件名。可以根据需要换成所需版本的 IOS。
```

`model = 3640` 路由器的型号是 3640，可以改成 dynamips 支持的其他型号设备，比如 3620、3725、7200 等。

`console = 3001`

该路由器使用的端口是 3001，如果远程访问此设备的控制台，可以 telnet 运行 CCNA 机架的计算机的 IP 地址 + 端口号。机架中的所有设备使用的端口号不能相同。

注意：如果是 7200 路由器，还有一个参数

`npe = npe-400` 网络处理引擎的类型是 npe-400，7200 路由器支持 3 种网络处理引擎，分别是 npe-225、npe-300、npe-400。

`ram = 128` 分配给该模拟器的内存是 128MB。

`confreg = 0x2142`

配置寄存器的值是 0x2142，路由器重启时不加载用户配置文件，也就是说，不管用户对路由器保存了任何配置，重启路由器后，配置都不被加载，这里主要是出于为大家节省时间考虑。一般的实验设备使用的都是这个值。如果需要路由器重启时加载用户保存的配置文件，可以把该值改成 0x2102，工程中的路由器使用的都是这个值。

`exec_area = 64` 可选参数，利用主机内存的一部分来加快执行。

`mmap = false` 可选参数，若不用 mmap=false，启动和关机会很慢，对运行速度也有不小的影响。

`slot1 = NM-16ESW`

插槽 1 中插入的是一块有 16 个端口的以太网模块。哪个插槽支持什么样的模块，模块上配置什么样的端口等，根据设备型号的不同会有差异，详细情况可以查询“<http://dyna-gen.sourceforge.net/>”。

`f1/1 = SW2 f1/2`

SW1 的 Fa1/1 口接 SW2 的 Fa1/2 口，在 SW1 上已经体现了 SW1 的 Fa1/1 口和 SW2 的 Fa1/2 口之间的连接，在 SW2 上就不需要再标明 SW2 的 Fa1/2 口接 SW1 的 Fa1/1 口了。也就是说一个连接，只要在一个设备上标明就可以了。

`f1/2 = SW2 f1/1` SW1 的 Fa1/2 口接 SW2 的 Fa1/1 口。

`f1/3 = SW3 f1/1` SW1 的 Fa1/3 口接 SW3 的 Fa1/1 口。

`f1/4 = PC1 f0/0` SW1 的 Fa1/4 口接 PC1 的 Fa0/0 口。

`f1/5 = PC2 f0/0` SW1 的 Fa1/5 口接 PC2 的 Fa0/0 口。

`f1/6 = R1 f2/0` SW1 的 Fa1/6 口接 R1 的 Fa2/0 口。

省略部分内容

`[[ethsw SW4]]`

SW4 是不可管理交换机，仅提供设备之间的连接，可以想象成二层交换机，该交换机有 5 个端口，前 4 个端口分别被 R1、R2、R3 所使用，最后一个端口连接的是获取到的物理网卡的参数。

`1 = access 1`

`2 = access 1`

`3 = access 1`

`4 = access 1`

`10 = access 1 NIO_gen_eth:\Device\NPF_{D9D333A4-CF15-4A3D-BC07-9D F5F0DD0872}`



4.2 路由器简介**

本节介绍路由器的基本硬件组成、路由器的引导过程、路由器的功能等。

4.2.1 路由器的基本硬件组成**

Cisco 路由器系列包含各种类型的路由器产品，尽管这些产品的处理能力和所支持的接口数目具有相当大的差异，但它们都由相似的核心硬件所组成。尽管微处理器（CPU）、ROM 和 RAM 的数目及所使用的端口、介质转换器的数量和方式会因产品类别的差异而不同，但每一个路由器均含有相似的硬件。

1. 中央处理器（CPU）

CPU 执行操作系统的功能，包括系统初始化、路由和交换功能等。

2. 闪存（Flash Memory）

闪存是一种可擦写的非易失性存储器，被用来保存路由器的操作系统，也就是 IOS。在

大多数型号的路由器上，闪存用来保存路由器的 IOS，当路由器启动时，IOS 被拷贝到 RAM 中；一些老型号路由器的 IOS 可以直接在闪存中运行。闪存由 SIM 或 PCMCIA 卡组成，可以被升级到更大的存储空间。只要有足够的有效空间，闪存中可保存多于一个操作系统的映像，这对于测试新的系统映像是很有用的。

设备断电或重启后，闪存中的内容不会丢失。

3. 只读存储器 (Read Only Memory, ROM)

ROM 中存储了那些不需要被更改或更新的内容，包括：

- Bootstrap instructions (引导程序)；
- Basic diagnostic software (基本诊断程序)；
- Scaled-down version of IOS (缩小版的 IOS)。

设备断电或重启后，ROM 中的内容不会丢失。

4. 随机存取存储器 (Random Access Memory, RAM)

RAM 用来保存路由表，执行包缓冲，并对那些因某一端口超载而不能直接输出的包进行排队。另外，RAM 可缓存 ARP 协议中地址映射的信息，即 ARP 表。

当设备在运行时，RAM 用来存储一些临时的指令和数据，包括：

- **Operating System** (运行的操作系统)：在路由器启动的时候，Cisco IOS (Internetwork Operating System, 互联网操作系统) 被复制到 RAM 中运行。
- **Running-config** (运行配置文件)：存储路由器 IOS 当前正在运行的配置命令的文件。除少数以外，路由器上的所有配置命令都存储在运行配置文件中，称为运行配置。
- **IP Routing Table** (IP 路由表)：存储直接连接和远程网络的信息，用来决定最佳的数据包转发路径。
- **ARP Cache** (ARP 缓存)：缓存了 IPv4 到 MAC 地址的映射，类似于计算机上的 ARP 缓存，这样可减少地址解析消息的数量，并提高与路由器相连的局域网的通信能力。ARP 缓存用于路由器的局域网接口，如以太网接口，在串行的广域网接口上是没有 MAC 地址的，也不用 ARP 缓存。
- **Packet Buffer** (包缓冲区)：当接口收到数据包或数据包离开接口时，数据包都会被暂时存放在一个缓冲区中。

设备断电或重启后，RAM 中的内容全部丢失。

5. 非易失性随机存取存储器 (NonVolatile RAM, NVRAM)

NVRAM 即使在断电的时候仍保留其中的内容。路由器使用 NVRAM 来保存启动配置文件 (Startup-config)，所有对配置文件的改变都保存在 RAM 中的运行配置文件中 (Running-config)，并立即发生作用。如果希望路由器断电或重启后，所做的修改仍然起作用，需要对运行的配置文件进行保存，也就是把改变保存到启动配置文件中。

设备断电或重启后，NVRAM 中的内容不会丢失。

6. 输入/输出端口 (Input/Output, I/O)

I/O 端口就是数据包进出路由器所通过的端口 (本书中的很多地方也称端口为接口，端口和接口所指相同，只是习惯上的叫法有些差异而已)。每个 I/O 端口与一个特定介质转换器相连，特定介质转换器为各种特定的介质，如以太网、令牌环局域网、RS-232 或 V.35 广

域网提供物理上的转换接口。

在 Cisco 术语里, 各种路由器功能(如路由协议更新和访问控制列表)都与某个接口相关联。可以使用“show interface”命令来显示路由器中所有接口相关的信息。

如果在插进路由器的一个槽中的通用适配卡上有一组端口, 例如在 7500、7200、3600 和 2600 型号的模块化路由器中, 下述引用的形式用于指定一个特定的串行端口:

```
interface serial slot#/port#
```

除了串行端口, 其他包括以太网、快速以太网、令牌环的端口也以相似的方式指定。运行 Dynamips 的 CCNA 模拟机架, 以后如不特别说明, 所说的机架均指 Dynamips 的机架。开启路由器 R1, 再执行“telnet R1”, 登录到 R1 的控制台, 在特权模式下使用“show ip interface brief”命令来显示路由器上当前激活或未激活的网络接口, 如图 4-2-1 所示。

Interface	IP-Address	OK?	Method	Status	Prot
FastEthernet0/0	unassigned	YES	unset	administratively down	down
Serial1/0	unassigned	YES	unset	administratively down	down
Serial1/1	unassigned	YES	unset	administratively down	down
Serial1/2	unassigned	YES	unset	administratively down	down
Serial1/3	unassigned	YES	unset	administratively down	down
FastEthernet2/0	unassigned	YES	unset	administratively down	down

图 4-2-1 显示路由器上的所有网络接口

在一些设备中, 在 1 个端口适配器卡上可以存在多个端口, 而多个端口适配器卡可以安装在 1 个插槽中, 因而上述引用的格式发生了变化。在这种情况下, 下述命令格式将用来引用一个特定的串行端口:

```
interface serial slot#/port-adapter#/port#
```

回想在图 4-1-2 中, 路由器的接口有 FastEthernet 0/0 和 Serial 0/0/0 的表现形式。

4.2.2 路由器的引导过程***

当打开路由器的电源后, 它执行 4 个主要的步骤: 执行 POST, 装入 Bootstrap 程序, 定位和装入 IOS, 定位和装入启动配置文件或进入 Setup 模式。如图 4-2-2 所示是路由器初始化过程中所执行的主要功能的一个流程图。

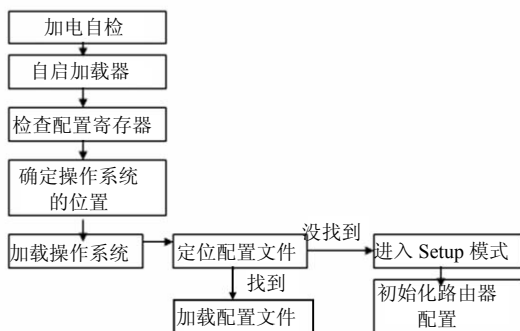


图 4-2-2 路由器的初始化过程

1. 执行 POST

几乎所有的路由器都需要执行 POST (Power-On Self Test, 加电自检), 加电自检被用来测试路由器的硬件。当路由器打开电源后, 它执行一系列诊断测试来校验其 CPU、RAM 和 NVRAM。当加电自检完成后, 路由器开始加载引导程序。

2. 加载引导程序 (Bootstrap)

POST 完成后, 引导程序被从 ROM 中拷贝到 RAM 中, CPU 开始执行引导程序中的指令。引导程序的主要功能就是定位 IOS, 并把 IOS 加载到 RAM 中。

3. 定位和加载 IOS

操作系统文件, 也叫 IOS。操作系统文件包含一系列规则, 这些规则规定如何通过路由器传送数据, 管理缓存空间, 支持不同的网络功能, 更新路由表和执行用户命令等。同一型号的路由器也有很多版本的 IOS, 不同版本的 IOS 支持的功能不同, 比如是否支持 IP 高级特性、是否支持安全特性、是否支持语音特性等。基本功能的 IOS 支持的功能较少, 但对硬件的要求相对较低, 尤其是内存。不同版本的 IOS 对内存的需求也是不一样的, 读者可以根据实际应用选择适合的 IOS 版本。

在加载 IOS 之前, 首先需要确定从哪里加载 IOS, 这是因为镜像文件可能放在闪存或 ROM 中, 甚至可能在网络上。为了找到操作系统的镜像文件放在哪里, 引导程序会检查配置寄存器的值。该值可以由硬件跳线或软件来设置, 这与路由器的型号有关。寄存器的设置指定了操作系统所在的位置并定义了其他设备的功能, 如路由器怎样响应控制台键盘的击键, 以及是否将自检的信息显示到控制终端上等。

现在多数型号路由器的配置寄存器是存储在 NVRAM 里的一个 16 位的值, 它并不是一个物理实体。在一些较老型号的路由器中, 配置寄存器是一个具有 16 针的跳线, 这是寄存器术语的起源。无论是软件还是硬件配置的寄存器, 最后的 4 位 (若是硬件寄存器, 则是跳针) 指明引导字段, 引导字段告诉路由器配置文件的所在地。软件寄存器以 4 位十六进制数字表示, 如 0x2142, 0x 表示的是十六进制数。每个十六进制数字代表 4 位二进制数, 所以从右边数起的第一个数字即为引导字段。引导字段的取值范围可以是 0~15, 在 0x2142 中, 引导字段的值为“2”。表 4-2-1 列出了路由器是如何解释启动域中的数值的。

表 4-2-1 路由器启动域中的数值

自启域值	路由器的解释
0	自动从 ROM 启动
1	RXBOOT 模式, 如果有 Mini IOS, 则加载
2-F	为 boot system 命令, 检查在 NVRAM 中的配置

当引导程序读取了配置寄存器的值后, 就知道了应从哪里加载操作系统的镜像, 并把它加载到 RAM 中。在大多数情况下, 启动域取值为“2”, 这将使路由器在 NVRAM 中查找启动的命令, 如果找到 boot system 命令, 就使用 boot system 命令中规定的方式引导。该命令的写法如下:

```
Router(config)#boot system flash flash:c1841-ipbase-mz.123-14.T7.bin
路由器默认加载闪存中的第一个 IOS 文件, 如果闪存中有多个 IOS 文件, 可以使用该命令加载指定的 IOS 文件。
Router(config)#boot system flash tftp://192.168.1.2/c1841-ipbase-mz.123-14.T7.bin
指定路由器从 TFTP 服务器加载 IOS 文件。
```

如果在 NVRAM 中找不到 boot system 命令, 或者 boot system 命令引导失败, 路由器将加载在闪存中的第一个镜像文件。如果闪存中也无有效操作系统的镜像文件或根本找不到闪存, 则路由器会尝试通过向广播地址发送 TFTP 请求操作系统镜像, 从 TFTP 服务器上加载镜像文件。

如果 IOS 加载失败, 一个缩小版 (Scaled-down version) 的 IOS 被从 ROM 拷贝到 RAM 中, 这个版本的 IOS 用来帮助诊断不能装入完整版 IOS 的原因。

4. 定位和装入配置文件 (Startup-config)

配置文件由管理员创建, 包括接口的地址、路由信息、密码和其他一些配置。其中, 存放的配置内容由操作系统解释, 操作系统指示路由器如何完成其中的各种功能。例如, 配置文件可以定义一个或多个访问控制列表, 并要求操作系统设置不同的访问控制列表来访问不同的接口, 以提供流入该路由器的包的控制级别。尽管配置文件定义了如何完成影响路由器运行的各种功能, 但实际上是由操作系统来完成这些工作的, 这是因为操作系统解释并响应配置文件中所陈述的要求。

IOS 加载成功后, 路由器查找保存在 NVRAM 中的配置文件。如果找到了, 路由器把它拷贝到 RAM 中并执行, Startup-config 被拷贝到内存中后叫做 Running-config, 这使得路由器可以根据预定义的网络环境开始工作。如果 NVRAM 中不存在配置文件, 路由器可能还会搜索 TFTP 服务器, 试图从 TFTP 服务器上加载配置。

若路由器加载配置文件失败, 路由器会显示 “Would you like to enter the initial configuration dialog?[yes/no]:”, 如果回答 “yes”, 则进入初始配置对话模式, 按照预定顺序的提问来进行配置; 如果回答 “no”, 则进入命令行配置模式, 路由器提示 “Press RETURN to get started!”, 按回车键继续, 路由器会显示一些接口信息, 并出现 “Router>” 提示符。命令配置功能强大, 本书中主要使用命令行配置模式。

当操作者将配置信息存储在 NVRAM 上时, 下次路由器重启时将加载保存在 NVRAM 中的配置。若把配置寄存器从右数起的第二位的数值置为 “4”, 则路由器在启动时会忽略 NVRAM 中的内容, 这项功能可在恢复路由器的密码时使用, 实际中被更多地使用在实验环境中, 一个学员完成实验后, 下一个学员重启设备, 路由器启动时不会加载任何配置。CCNA 机架中所有路由器的配置寄存器值都被设成 0x2142, 启动时不加载配置文件, 如果想加载用户的配置文件, 则把 “\labini\ccna.net” 中对应设备的 0x2142 改成 0x2102。

配置文件的内容以文本形式保存, 因此, 其内容可在路由器控制台终端或远程终端上显示。这一点十分重要, 因为当在一台与网络相连接的计算机上创建并修改配置文件, 然后使用 TFTP 协议将文件加载到路由器时, 由于所使用的文本编辑器或字处理器通常会在保存的文件中加入一些控制字符, 致使路由器不能识别文件的内容。所以, 当使用文件编辑器或字处理器创建并维护配置文件时, 切记把文件保存为 ASCII 码的文本文件 (.txt)。配置文件保存后, 就可存储在 NVRAM 中, 并在每次路由器初始化时被加载到内存的高端地址空间中。

5. 路由器启动时的输出信息

在 Packet Tracer 中, 打开 4.1.1 节中建立的 First.pkt 文件, 单击两台路由器中的任何一台路由器, 再选择 “命令行” 标签, 即可看到路由器的启动过程。读者也可以关闭路由器的电源, 然后再打开路由器的电源, 让路由器重新启动, 观看路由器的启动过程。路由器

启动时所产生的输出信息如下（斜体部分是注释）：

! 注意：本书中所有阴影部分都表示路由器的输出或配置命令，除非特别说明，所有阴影部分中的斜体字都表示作者添加的注释。如果只是路由器的输出而没有注释，将不用阴影显示。

```
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Self decompressing the image :   IOS 文件被拷贝到 RAM 中，因为使用的 IOS 文件是压缩的，这里
                                执行的是解压缩。
#####System Bootstrap, Version 12.3(8r)T8, RELEASE
SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Self decompressing the image :
##### [OK]
省略部分
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7, RELEASE SOFTWARE
(fc2)   这里显示的是 IOS 文件的版本信息。
省略部分，接下来显示的是路由器的内存，接口等信息。
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7, RELEASE SOFTWARE
(fc2)

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:   NVRAM 中没有找到配置文件，提示是否要进
入对话框配置模式。
```

4.2.3 show version 命令***

show version 命令可以被用来检验和排除路由器基本硬件和软件问题。在 Packet Tracer 中，打开 4.1.1 节中建立的 First.pkt 文件，单击两台路由器中的任何一台路由器，再选择“命令行”标签，使用 show version 命令进行查看。显示如下：

```
Router>show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7, RELEASE SOFTWARE
(fc2)   IOS 文件的版本信息。
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 15-May-06 14:54 by pt team
ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Bootstrap 自引导程序的版本。

Router uptime is 7 minutes   路由器运行了多长时间。
System returned to ROM by reload at 02:07:35 UTC Wed Jun 11 2008
路由器本次启动的原因和时间，这里显示路由器是被管理员使用 reload 命令重启的。
System image file is "flash:c1841-ipbase-mz.123-14.T7.bin"   系统是从 flash 中加载的，
                                                              以及 IOS 的名字。

下面显示的是一些版权和帮助信息。
This product contains cryptographic features and is subject to United
```


States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
 路由器型号和内存的数量, 114688K 被用来存储 IOS 和其他系统程序, 16384K 专门被用来作为数据包缓存, 两者加起来是总共的内存数量, 即 128M。

Processor board ID FTX0947Z18E

主板信息。

M860 processor: part number 0, mask 49

CPU 信息。

2 FastEthernet interfaces

路由器接口信息。

2 Serial(sync/async) interfaces

路由器接口信息。

191K bytes of NVRAM. NVRAM 的空间, NVRAM 被用来保存 Startup-config。

31360K bytes of ATA CompactFlash (Read/Write) Flash 的空间, 闪存被用来存储路由器的 IOS 文件。

Configuration register is 0x2102

配置寄存器的值。

4.2.4 路由器外观*

CCNA 考试中推荐使用的路由器型号是 Cisco 1841, 它是一种成本相对较低的 ISR (Integrated Services Routers, 集成服务路由器), 适合用于中小型企业和小型企业的分支机构。它集成了数据、安全和无线服务等特点。

1. 路由器的前面板

如图 4-2-3 所示是 Cisco 1841 路由器的前面板, 其上面有两个 LED (Light Emitting Diode, 发光二极管) 指示灯:

- System Power LED, 设备的电源指示灯, 一般是持续绿色。
- System Activity LED, 发送或接收任何数据包, 以及监控系统有活动时, 该灯闪烁。



图 4-2-3 Cisco 1841 路由器的前面板

2. 路由器的后面板

如图 4-2-4 所示是 Cisco 1841 路由器的后面板。其上面有:

- **4-port Cisco EtherSwitch:** 路由器上的交换模块, 有 4 个端口, 均是 10/100Mb/s 自适应端口。
- **Compact flash module:** 也称 CF 卡, 最初是一种用于便携式电子设备的数据存储设备。
- **Fa0/0 和 Fa0/1:** 路由器上的快速以太网接口。
- **Console:** 控制台端口, 使用专用配置线缆直接连接至计算机的串口, 利用终端仿真

程序（如 Windows 下的“超级终端”）对路由器或交换机进行初始配置。路由器的 Console 端口多为 RJ-45 端口。

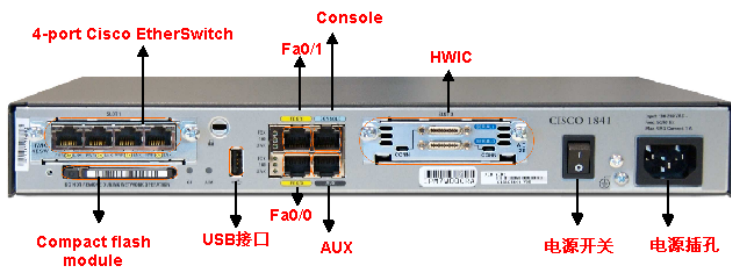


图 4-2-4 Cisco 1841 路由器的后面板

- **AUX**（Auxiliary Port，辅助配置端口）：AUX 端口为异步端口，可以用于拨号上网。除了通过 Console 端口对路由器进行配置外，还可以使用 AUX 借助 Modem 对路由器进行远程配置。当需要通过远程访问的方式实现对路由器的配置时，就需要采用 AUX 端口了。AUX 端口在外观上与 Console 一样，只是里面所对应的电路不同。
- **HWIC**（High-speed WAN Interface Card，高速广域网接口卡）：主要用于广域网的连接，图中的模块上有两个串行接口。

3. 路由器的接口

在图 4-2-4 中，可以看到路由器的几种不同接口。路由器接口可以分为管理接口和路由接口。

（1）**管理接口**。通过管理接口对路由器的访问也称为带外管理（Out-Of-Band，简称 OOB）。路由器通过管理接口来物理连接路由器，进行初始配置。不同于以太网和串行接口，管理接口不用于包转发。最常见的管理接口是 Console 端口，另一个管理接口是 AUX 端口。

（2）**路由接口**。通过路由接口对路由器的访问也称为带内管理（In-Band，简称 IB）。路由器使用路由接口来接收和转发数据包，路由器有多种类型的路由接口来连接物理网络。比如，路由器使用快速以太网接口来连接局域网，使用其他类型的广域网接口来连接 T1、DSL 和 ISDN 等。路由接口用来连接不同的 IP 子网，路由器的每一个接口必须属于不同的 IP 子网。路由接口可以被分成：

- **局域网接口**：类似于计算机的以太网网卡，路由器的以太网接口也有一个二层的 MAC 地址，与一般计算机的工作原理相同，也发送 ARP 请求包，应答 ARP 查询，并维护 ARP 缓存。
- **广域网接口**：广域网接口被用来连接外部网络，经常是跨越一个大范围的网络，二层使用不同的封装协议，诸如 PPP（Point-to-Point）、帧中继（Frame Relay）和 HDLC（High-Level Data Link Control，高级链路控制协议）。



4.3 路由器的一般操作***

本节介绍路由器的基本配置，包括路由器的控制台连接、路由器 CLI（Command Line Interface，命令行接口）、路由器的配置模式、路由器命名、密码配置、接口配置、旗帜配

置、保存和检验路由器的配置。

4.3.1 控制台连接***

在路由器第一次从包装盒取出加电后，路由器使用的是默认的出厂配置，路由接口也没有配置 IP 地址。路由器不像计算机，既没有键盘，也没有显示器，此时需要借助计算机使用配置线缆通过 Console 端口对路由器进行初始化配置。

1. 连线

把厂商提供的配置线缆（全反电缆）的一端接入路由器标志有“Console”的端口，另一端将 RJ-45 接到 DB-9 的转接器，把转接器接在计算机的 COM 口上，如图 4-3-1 所示。现在更多的配置线缆都是一根整线，转接头和全反电缆已经固定在一起了。

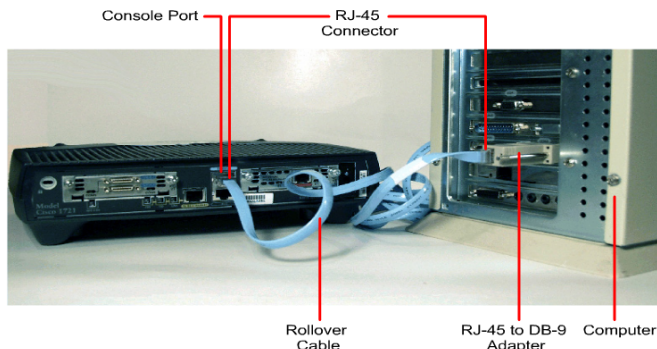


图 4-3-1 路由器初始配置接线图

2. 访问控制台

有多种通信程序可以用来通过 Console 端口高效地访问路由器，比如 Secure CRT 就是一款方便、灵活、功能全面的通信程序。这里出于方便考虑，使用 Windows 操作系统自带的超级终端。

当电缆正确连接后，在计算机上单击“开始”→“程序”→“附件”→“通信”→“超级终端”，如果是第一次使用超级终端，还会要求输入区号，接下来打开“连接描述”窗口，为新的连接指定一个名字“CCNA”，接下来打开如图 4-3-2 所示的“连接到”窗口，选择对应的 COM 口。

由于是直接用电线连接计算机和路由器的控制台端口，设置“连接时使用”选项来说明该连接使用的是直接的串行通信口，现在很多新款笔记本电脑都不再集成 COM 口，解决的办法就是买一根 USB 转 COM 口的转接线缆。在如图 4-3-2 所示的例子中，选择了 3 号串行通信口（COM3）。

一旦选择了适合直接连接的串行通信口并单击“确定”按钮，超级终端程序就会弹出一个对话框，来设置串行通信的参数。如图 4-3-3 所示的“端口设置”对话框，用来定义在计算机与路由器端口之间的通信设置，Cisco 路由器的 Console 端口默认设定为 9600 比特、8 数据位、无奇偶检验和 1 停止位。单击“确定”按钮，如果一切无误的情况下，此时已经可以通过超级终端配置路由器了。

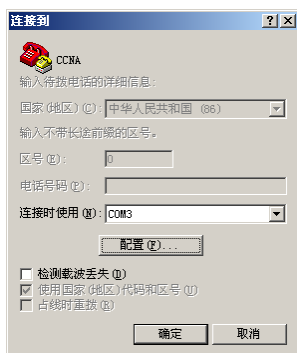


图 4-3-2 “连接到” 窗口

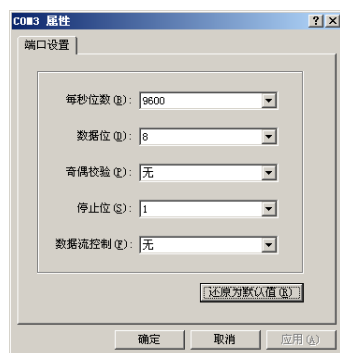


图 4-3-3 “端口设置” 对话框

4.3.2 Setup 模式*

路由器启动后，如果找不到启动配置文件，将出现 “Would you like to enter the initial configuration dialog? [yes/no]:” 提示，如果输入 “yes”，或在特权模式下输入 “Setup”，将进入 Setup 配置模式。

双击 CCNA dynamips 文件夹中的 “0.启动虚拟服务.bat”，并且实验结束前不要关闭该窗口；双击 CCNA dynamips 文件夹中的 “1.控制台 CCNA.cmd”，如图 4-3-4 所示，并在控制台窗口中输入 “start R1”，给路由器 R1 加电，然后输入 “telnet R1”，打开路由器 R1 的控制台窗口。

接下来的输出来自控制台端口：

```
Cisco 3640 (R4700) processor (revision 0xFF) with 77824K/4096K bytes of memory.
Processor board ID 00000000
R4700 CPU at 100MHz, Implementation 33, Rev 1.2
2 FastEthernet interfaces
4 Serial interfaces
DRAM configuration is 64 bits wide with parity enabled.
125K bytes of NVRAM.
8192K bytes of processor board System flash (Read/Write)
```



图 4-3-4 启动 CCNA 控制台

--- System Configuration Dialog ---

```
Would you like to enter the initial configuration dialog? [yes/no]: y
是否要继续配置对话？选择是或不是，这里选择的是“y”。
At any point you may enter a question mark '?' for help.
任何时候可以输入“？”获取帮助。
Use ctrl-c to abort configuration dialog at any prompt.
```

任何时候可以输入 Ctrl + C 组合键放弃配置并退出 Setup 模式。

Default settings are in square brackets '[']'.
方括号中显示的是默认配置，直接回车表示接受默认配置。

Basic management setup configures only enough connectivity

for management of the system, extended setup will ask you
to configure each interface on the system

基本管理的 Setup 配置可以为管理提供连接，扩展管理的 Setup 配置将会要求你配置系统的每一个接口。

Would you like to enter basic management setup? [yes/no]: y

要进行基本管理的 Setup 配置模式吗？

Configuring global parameters:

全局配置参数。

Enter host name [Router]:Cisco3640

输入路由器的名字，方括号中是默认值，如果接受，不需要重新输入，直接回车即可，这里输入 Cisco3640。

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.

加密的使能密码被用来保护访问特权命令和进入配置模式，这个密码输入后在配置文件中会被加密。

Enter enable secret: cisco123 输入加密的使能密码。

The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images. 没有加密的使能密码时，将会使用这个使能密码。

Enter enable password: cisco 输入使能密码。

The virtual terminal password is used to protect
access to the router over a network interface. 虚拟终端密码用来保护从网络对设备的访问。

Enter virtual terminal password: cisco 输入虚拟终端的密码。

Configure SNMP Network Management? [no]: y 要配置简单网络管理协议吗？

Community string [public]: 输入简单网络管理协议的团体字符串。

Current interface summary

当前的接口汇总。

Interface	IP-Address	OK?	Method	Status	Pr
FastEthernet0/0	unassigned	YES	unset	administratively down	do
Serial1/0	unassigned	YES	unset	administratively down	do
Serial1/1	unassigned	YES	unset	administratively down	do
Serial1/2	unassigned	YES	unset	administratively down	do
Serial1/3	unassigned	YES	unset	administratively down	do
FastEthernet2/0	unassigned	YES	unset	administratively down	do

Enter interface name used to connect to the
management network from the above interface summary: fastethernet0/0
输入从上面哪一个接口来管理网络，这里选择的是 fastethernet0/0，这里的接口命令不可缩写。

Configuring interface FastEthernet0/0:

配置网络管理接口。

Use the 100 Base-TX (RJ-45) connector? [yes]:

该接口是 100Mbps 的双绞线吗？

Operate in full-duplex mode? [no]:

操作在全双工模式吗？

Configure IP on this interface? [no]: y

要给接口配置 IP 地址吗？

IP address for this interface: 192.168.1.2

输入接口的 IP 地址。

Subnet mask for this interface [255.255.255.0] :

输入接口的子网掩码。

Class C network is 192.168.1.0, 24 subnet bits; mask is /24

The following configuration command script was created: 创建下面的配置命令脚本。

hostname Cisco3640

.....

省略部分

.....

end

[0] Go to the IOS command prompt without saving this config.

选项 0 放弃保存，退出配置模式。

[1] Return back to the setup without saving this config. 选项 1 放弃保存，重新执行 setup。

[2] Save this configuration to nvram and exit. 选项 2 保存配置，退出配置模式。

Enter your selection [2]:

输入您的选项。

setup 命令显示的一部分配置信息被从中删去，可以在每个项目的输入位置键入问号来获得在线帮助。一旦配置完成后，路由器会生成一个命令行脚本，来显示最近更改过的配

置项。此时，有 3 种选择：一是不保存改动，返回 IOS 命令提示行；二是不保存改动，返回到 Setup 模式重新再来；三是保存配置。在命令执行过程中，随时可以按“Ctrl+C”组合键终止 Setup 模式。

! 注意：本书中所有的实验都不使用配置对话，路由器启动后，询问“Would you like to enter the initial configuration dialog? [yes/no]:”，全部输入“n”，不使用 Setup 配置模式。

上面输入命令的方式叫 CLI（Command Line Interface，命令行接口），IOS 负责解释和执行输入的命令。

4.3.3 路由器的操作模式**

路由器的操作模式主要有：

(1) **用户（User）模式**。当用户登录到路由器后，就进入了用户命令模式，在本模式中系统提示符为“>”。如果用户先前已为路由器命名了，则路由器的名字将会位于“>”之前；否则，默认的 Router 将会显示在“>”之前。

路由器上默认有两级 EXEC 命令层次：用户级和特权级。用户级的权限级别是“1”，在用户模式下可以执行所有级别 1 和级别 0 的命令；特权级的权限级别是“15”，在特权模式下可以执行权限 0 到权限 15 的所有命令。在默认情况下，级别 0 包括 5 个命令：disable、enable、exit、help、logout，权限 2 到权限 14 都没有使用，管理员可以把某些命令的权限级别从 15 降到级别 2 到 14 中的某个级别，有关这方面的讨论已经超出本书的范围。

(2) **特权（Privileged）模式**。在提示符“>”之后输入 enable 命令，进入特权配置模式，CLI 提示符变成“#”，在特权模式下使用 disable 命令返回到用户模式。在特权模式下可以执行所有的命令，如更改路由器的时间，清除登录路由器的用户，查看路由器某方面的信息等。

```
Router>
Router>enable
Router#
Router#disable
Router>
```

(3) **全局配置（Global configuration）模式**。在特权模式下，输入命令“configure terminal”，进入全局配置模式，路由器的提示符改变为 Router（config）#，在全局配置模式下输入 exit 命令，返回到特权模式下。全局配置命令定义了系统范围的参数，包括更改路由器的名字和编辑访问控制列表等。下面的配置中斜体部分是注释。

```
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CCNA          hostname 命令用来更改路由器的名字。
CCNA(config)#exit
CCNA#
```

(4) **其他配置模式**。路由器中还有一些其他的配置模式，包括接口配置模式、路由配置模式、线路配置模式等。这里先介绍接口配置模式，路由和线路配置模式将在后面的章节中介绍。

接口配置模式：在全局配置模式下使用接口命令定义一个 LAN 和 WAN 接口的特征。进入接口的命令格式是：

```
interface type number
```

此处 type 指出配置的接口类型，图 4-3-5 中列出了当前路由器上支持的接口类型。后面的 number 是接口的编号，有时接口编号的前面还要加上插槽的编号，更复杂的格式是：

```
interface type slot#/port-adapter#/port#
```

接口的输入形式与具体的路由器型号和插槽有关，可以在特权模式下使用“show running-config”命令查看路由器上的接口数量和类型。

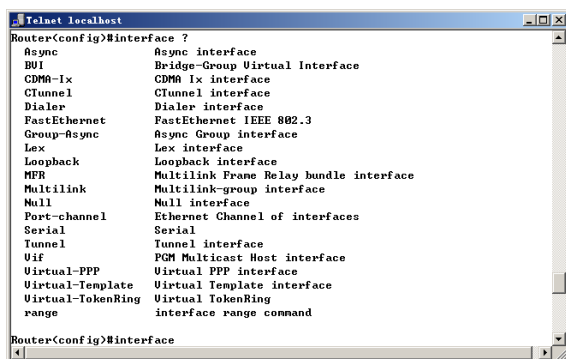


图 4-3-5 路由器上支持的接口类型

```
CCNA#show running-config
省略
hostname CCNA
省略
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface Serial1/0
no ip address
shutdown
serial restart-delay 0
省略
end

CCNA#
```

从上面的输出中可以看出，路由器上有一个“FastEthernet0/0”接口，使用 interface 命令进入这个接口，使用 exit 命令返回到全局配置模式下，使用 end 命令或“Ctrl+Z”组合键返回到特权模式下。

```
CCNA(config)#
CCNA(config)#interface fastEthernet 0/0
CCNA(config-if)#exit
CCNA(config)#
CCNA(config)#interface fastEthernet 0/0
CCNA(config-if)#^Z
CCNA#
```

4.3.4 命令行接口**

1. 在线帮助

CCNA 中完成的大量配置都是在 CLI 中完成的，初学者一定要掌握 CLI 的使用。思科

IOS 提供 CLI 的在线帮助功能，用户可以在任何情况下输入“？”来获取在线帮助。比如忘记 enable 单词的写法，只知道第一个字母是“e”，在路由器用户模式下输入：

```
CCNA>e?
enable  exit

CCNA>e
```

在线帮助显示在当前模式下，以字母“e”打头的命令有两个，分别是 enable 和 exit。

有时帮助或输出信息一屏显示不完，路由器将在页面的最下面提示“--More--”，如图 4-3-6 所示，此时可以按回车键滚动一行，按空格键滚动一屏，按任意键退出。

IOS 负责解释和执行用户输入的命令，如果用户输入错误信息，路由器提示输入非法，并使用“^”定位输入出错的位置。如图 4-3-7 所示，用户输入“configure terminal”命令输错，少输入了一个字母“r”，CLI 的在线帮助提示出错，并定位出错的位置。

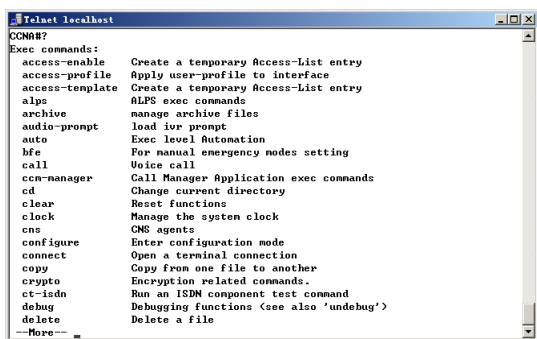


图 4-3-6 多屏显示

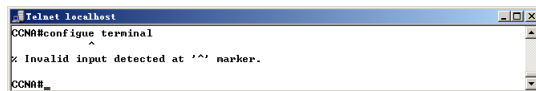


图 4-3-7 输错命令提示

2. 命令的简写

在路由器上输入一个命令时，并不需要将整词输入。一般来说，命令的 3~4 个字母就可以使路由器分清所用的命令，并执行相应的动作。例如，以下命令：

```
Router>enable
```

能简写为：

```
Router>en
```

这样就很容易输入了。当有疑问时，首先输入命令最前面能记得清的字母，然后再加一个“？”，这样可得到路由器的上下文在线帮助，路由器将会显示与所有字符相匹配的命令，然后，用户可以输入足够多的字符来完成命令的输入。比如，输入 enable，以字母“e”打头的命令有 2 个：enable 和 exit，如果再输入一个字母“n”，则以“en”打头的命令只有“enable”，输入“en”直接回车就可以了，如果想把命令补全，此时可以按“Tab”键。通过使用内嵌的上下文敏感的帮助系统，就是一个 Cisco 的初学者也能确定正确的命令语法。

3. CLI 快捷键和高级编辑功能

通过使用快捷键可以加快对 CLI 命令的输入和编辑。表 4-3-1 中列出了一些常用的、值得使用的快捷键。

表 4-3-1 CLI 快捷键及功能描述

快 捷 键	功能描述
Tab	补全命令的输入，对一些没有二义性的命令，可以使用 Tab 键把后面的部分补全
Ctrl + K	删除从光标到行尾的所有字符
Ctrl + U 或 Ctrl + X	删除从行开始到光标处的所有字符
Ctrl + A	移动光标到行的开始处，Cisco 中很多命令的取消都是在行的最前面加上 no，可以使用该组合键快速地把光标移动到行首
Ctrl + E	移动光标到行的末尾
向上箭头或 Ctrl + P	调出前一条命令
向下箭头或 Ctrl + N	调出后一条命令
Ctrl + R、I 或 L	重新在新行上输入被控制台消息影响的输入，比如： CCNA(config-if)#ip add 1.1.1.1 *Mar 1 02:14:40.315: %LINK-5-CHANGED: Interface Serial1/1, changed state to administratively down 255 输入的命令“ip add 1.1.1.1 255”被控制台消息影响，使可读性变差，可以使用该组合键在新的一行中输出已经输入的命令，如下所示： CCNA(config-if)#ip add 1.1.1.1 255
Ctrl + C	在配置模式下，放弃当前的操作返回到特权模式下。如果是在 Setup 模式下，则是放弃当前的配置，退出 Setup 模式
Ctrl + Z	在配置模式下，放弃当前的操作返回到特权模式下
Ctrl + Shift + 6	放弃 DNS 名称查找、连续的 ping 包、Traceroute 操作等

可以在特权模式下使用：

```
CCNA#terminal editing      打开高级编辑功能。
CCNA#terminal no editing   关闭高级编辑功能。
```

4. 配置历史命令缓存

输入命令时，对于很长的一串字符，中间输错了一个字母，或者一条重复的命令稍后又要再次输入，这时就可以使用历史命令缓存功能。思科路由器上默认启用了历史命令缓存功能，只需在命令行接口按上下箭头键，即可调入历史命令。路由器默认缓存了最近 10 次输入的命令，读者可以使用下面的命令修改缓存的历史命令的记录数。

```
Router#terminal history size ?      历史命令缓存记录数，最大可以是 256 条。
<0-256> Size of history buffer

Router#terminal history size 20     这里把命令缓存记录数设成 20 条。
```

使用下面的命令查看缓存的历史命令：

```
Router#show history
```

使用下面的命令关闭历史命令的缓存功能：

```
Router#terminal no history
```

使用下面的命令打开历史命令的缓存功能：

```
Router#terminal history
```

使用下面的命令把历史记录缓存数恢复成默认的 10 条：

```
Router#terminal no history size
```

4.3.5 路由器常用配置***

接下来介绍路由器的常用配置，包括：路由器的命名、配置旗帜消息、设置路由器的时间、配置路由器的接口、配置路由器的密码等。

1. 路由器命名

路由器的命名与重命名是通过命令 `hostname` 完成的。因为命令 `hostname` 是一个全局配置命令，所以用户必须在全局配置模式下才能对路由器名进行设置或重新设置。在实际中，路由器名称应有某种意义，特别是当用户有一个复杂的网络时。例如第 2 层楼第 3 个设备间，路由器的管理 IP 地址是 192.168.1.16，则路由器的名字可以表示成 2-3-16，看起来非常直观。

2. 旗帜创建

当执行某种初始化动作时，显示所谓“旗帜”信息。在一个 Cisco 路由器环境中，用户可以看到几种不同的旗帜消息。图 4-3-8 举例说明了 `banner` 命令后跟参数“?”所显示的路由器所支持的旗帜消息。在图 4-3-8 中，`LINE` 不是一个旗帜选项，而是用户输入旗帜文本消息的方式。例如，为了显示消息 `hello`，用户在此单词前后需输入一对分界符，如“#”，因此，这个线路命令输入变为 `#hello#`。注意要小心选择作为分界符的字符，它们不能在旗帜消息中被使用。

`banner exec` 命令是当一个线路命令激活时用来显示消息的，比如来了一个虚拟终端(VTY)连接或一个相似的 EXEC 过程时；当用户需要一个如 `telnet` 的登录连接路由器时，命令 `banner login` 也导致消息的显示。这样，命令 `banner login` 的消息比 `banner exec` 命令消息要早。其他的 `banner` 命令选项如图 4-3-8 所列，包括 `incoming`、`motd`、`prompt-timeout` 和 `slip-ppp`。

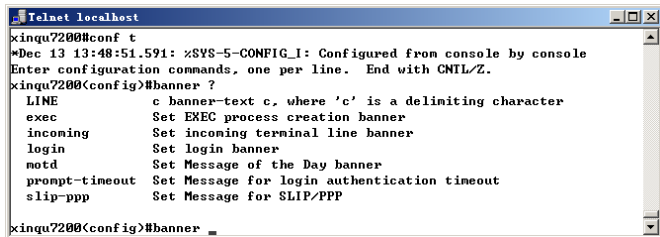


图 4-3-8 旗帜信息

当一个从网络来的 `incoming` 连接初始化时，显示 `banner incoming` 消息。`motd` 子命令允许用户说明日期信息，当任何时候与路由器任何类型的连接发生时，`motd` 旗帜将显示出来，因此，可以考虑用它来传送影响用户的信息。例如，如下命令：

```
Router(config)#banner motd * This router will be power off from 14:00 to 20:00 today*
```

当用户连接到路由器时，提示这台路由器今天从 14 点到 20 点将被关闭。当一个登录认证过程超时，`prompt-timeout` 子命令显示一个消息。最后，`slip-ppp` 子命令用来显示通过其他协议访问的消息。

注意到旗帜消息的显示是有特定顺序的，而并不管用户设置旗帜信息命令的次序。如果有旗帜 `motd`，那么它的信息将会最先显示；接着，若配置了旗帜命令 `incoming`，它的旗帜信息将跟着显示；如果有一个用户登录，而又配置了旗帜命令 `EXEC`，它的旗帜信息也会

显示出来。

使用加 no 的 banner 命令可以删除先前的一个条目，例如，在一个 banner login 命令之后输入一个 no banner login 命令，可以禁止先前的输入。在路由器任何命令前加上 no，对返回路由器的默认参数和清除前一个命令的影响是非常有效的。

3. 设置日期/时间

Cisco 路由器支持几个系统日历和时钟的命令，用户可以用 clock set 命令设置路由器的系统日历，在命令之后可以输入以下两种格式之一的时间和日期：

```
hh:mm:ss day month year
hh:mm:ss month day year
```

用户输入日期的天数时用数字形式，而用英文表示月份，系统自动识别两种不同格式的输入。下面两种输入方式均可：

```
Router#clock set 8:43:00 12 june 2008
Router#clock set 8:43:00 june 12 2008
```

上面设置的时间是 UTC 时间，比北京时间晚 8 个小时，为了和其他计时系统一致，最好改成北京时间，也就是东八区时间。使用 clock timezone 命令修改，如下所示把时区改成东八区：

```
Router(config)#clock timezone GMT +8
```

4. 配置路由器接口

路由器的接口有局域网接口和广域网接口之分，路由器的不同接口必须配置在不同的子网中。配置路由器接口的 IP 地址的命令如下：

```
Router(config)#int s1/1          配置路由器的广域网接口 serial 1/1。
Router(config-if)#description this port is link to internet 端口描述信息。
Router(config-if)#ip address 12.1.1.1 255.255.255.0      配置 IP 地址和子网掩码。
Router(config-if)#no shutdown 路由器的接口默认都是关闭的，需要使用 no shutdown 命令打开接口。
Router(config-if)#exit          返回到全局配置模式下，其实可以在一个接口下直接进入另一个接口，
而不需要返回到全局配置模式下。
Router(config)#int fa 0/0        配置路由器的局域网接口 fastethernet 0/0。
Router(config-if)#ip add 13.1.1.1 255.255.255.0          配置 IP 地址和子网掩码。
Router(config-if)#no shut        打开接口。
```

对于广域网接口还会涉及时钟和封装协议。广域网接口需要配置时钟提供同步，在实验的环境下，在电缆 DCE 端使用 clock rate 配置时钟，命令如下：

```
Router(config)#int s1/1
Router(config-if)#clock rate 64000
```

广域网的封装协议，将在广域网部分讨论。

！ 注意：在 CCNA 模拟机架上的所有路由器都不需要配置时钟，但在实际环境中或一些低端的路由器上，时钟有时是一个必须配置的参数。尤其在 CCNA 考试中一定不要忘记这一点。

Secondary 地址

路由器的一个接口可以配置多个 IP 地址，就像多数 Windows 操作系统一样，可以在一块网卡上添加多个 IP 地址，多个 IP 地址可以属于同一个 IP 子网，也可以属于不同的 IP 子网。使用的命令如下：

```
Router(config)#int fa 0/0          配置路由器的局域网接口 fastethernet 0/0。
```

```
Router(config-if)#ip add 13.1.1.1 255.255.255.0    配置 IP 地址和子网掩码。
Router(config-if)#ip add 31.1.1.1 255.255.255.0 secondary
配置该接口的第二个 IP 地址和子网掩码，类似的配置更多 IP 地址的命令也是在最后加上 secondary。
Router(config-if)#no shut    打开接口。
```

取消接口多个 IP 地址的命令要使用 “no ip address [ip] [子网掩码]” 的格式，简单地使用 “no ip address” 会删除该接口下的所有 IP 地址。

5. 配置路由器密码

为了保证路由器的安全，需要配置一些密码。

(1) **配置 Console 端口密码。**配置 Console 端口密码后，通过配置线缆连接到路由器时，需要输入密码。配置的命令如下：

```
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
```

(2) **配置特权密码。**也就是使能密码，从用户模式切换到特权模式的密码。配置命令如下：

```
Router(config)#enable password cisco
```

使能口令被显示为 cisco，当有人输入 enable 命令之后，必须提交使能口令。除了使能口令外，管理员还可以配置一个秘密使能口令，它的作用与标准的使能口令一样，但秘密使能口令以 MD5 的方式封装在配置文件中。当显示配置文件时，只能看到秘密使能口令的封装版本，这对于防止任何人通过获取路由器配置文件的复制件而推知秘密使能口令具有重要的意义。配置命令如下：

```
Router(config)#enable secret cisco123
```

！ 注意：当 enable password 和 enable secret 两个命令同时使用时，enable password 命令失效。还要注意输入密码时的前导空格被忽略，而末尾空格是有效的，比如输入一个 “cisco 空格” 的密码，将很难被发现。

(3) **配置远程登录密码。**这里的远程登录是指通过 Telnet 或 SSH 等对路由器的远程访问，也称 VTY（Virtual Type Terminal，虚拟终端类型）。思科路由器在默认情况下不允许从远程访问路由器，除非对路由器 VTY 进行配置，配置的命令如下：

```
Router(config)#line vty 0 4
配置虚拟终端用户 0 到 4，也就是配置 5 条线路，允许 5 个并发的登录，第一个远程登录的用户是 vty 0，
第二个是 vty 1，其余的依次类推。有的路由器允许的并发登录不止 5 个，模拟机架的路由器可以支持几百个
并发的连接。
Router(config-line)#password cisco
Router(config-line)#login
要求登录，这样用户登录时，需要提供前一条命令配置的密码，如果这里配置的是 no login，路由器远程登
录时将不需要密码，这样虽然方便，但却是非常不安全的，不推荐这样做。
```

对于 Console 和 VTY 线路上配置的口令都是明文显示，有一个命令 “service password-encryption” 用来对所有的密码进行加密，包括加密虚拟终端、控制台端口、使能密码，以及配置文件中的用户密码等。不过，这条命令的加密强度远弱于命令 enable secret，以至于很多在因特网上的自由软件在瞬间就可以破译该密码。如果要取消密码的加密，使用命令 “Router(config)#no service password-encryption”，但这条密码并不能还原之前被 “Router(config)#service password-encryption” 加密的密码，也就是说，这种方法是不可逆的。

6. 配置路由器的远程登录

运行 Dynamips 机架中的路由器 R1 和 R2，配置 R1 和 R2，使 R1 可以远程登录到 R2，IP 地址和连线情况如图 4-3-9 所示。

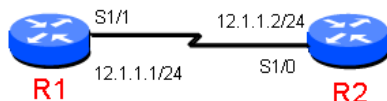


图 4-3-9 配置远程登录

(1) 路由器 R1 的配置如下：

```
Router>en                                从用户模式进入特权模式。
Router#conf t                             从特权模式进入全局配置模式。
Router(config)#host R1                    更改路由器的名字。
R1(config)#int s1/1                       配置串行接口 S1/1。
R1(config-if)#ip add 12.1.1.1 255.255.255.0
配置 IP 地址和子网掩码，如果是配置一些低端的路由器，在串行线缆 DCE 端要设置时钟，CCNA 考试中一定不要忽略这一点。这里使用的模拟路由器可以自动配置时钟，现实中的很多新款路由器也可以自动在 DCE 端配置时钟。
R1(config-if)#no shut                    打开端口。
```

(2) 路由器 R2 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#enable password cisco        配置使能密码，否则路由器将不允许远程用户进入特权模式。
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#line vty 0 4              配置 VTY 线路，以允许远程登录。
R2(config-line)#password cisco          远程登录的密码是 cisco。
R2(config-line)#login
R2(config)#line console 0               配置 Console 端口。
R2(config-line)#logging synchronous
配置日志同步，虽然不是必需的步骤，但却相当实用。当正在输入一行命令时，被屏幕弹出的日志消息打断，虽然不影响用户继续输入，可多数用户都不太确认前面输入到哪里了。通过配置日志同步，路由器将在新的一行上输出前面用户已输入的字符，相当于自动执行“Ctrl + R”组合键。
```

！ 注意：这里的 telnet 12.1.1.2，通过路由器 R1 的 S1/1 口对路由器 R2 进行访问，也称为虚拟终端类型（VTY）访问，VTY 可以同时提供多个连接。而在 CCNA 机架的控制台中，可能通过 telnet R2 对 R2 进行配置，CCNA 控制台上连接的是 R2 的控制台（Console 端口），Console 端口同时只能提供一个连接。因为虚拟路由器都看不见，更无法连接 Console 端口，在 CCNA 机架的控制台上，telnet R2 相当于连接到虚拟路由器 R2 的 Console 端口，通过配置线对 R2 进行初始化配置，以后就可以通过网络线对 R2 进行远程配置了。

(3) 测试，在路由器 R1 上登录 R2，如图 4-3-10 所示。

- 第 1 行，使用“telnet 12.1.1.2”，在路由器 R1 上登录 R2。
- 第 4 行，提示输入路由器 R2 配置的 VTY 密码。输入远程登录密码，屏幕不显示输入的密码，输入完密码后按回车键继续。
- 第 5 行，输入 en 进入路由器 R2 的特权模式。
- 第 6 行，输入路由器 R2 上的使能密码。
- 第 7 行，输入 conf t 进入路由器 R2 的全局配置模式。
- 第 9 行切换到第 10 行，在远程登录的路由器 R2 上同时按下组合键“Ctrl + Shift + 6”，松开 3 个键后，马上按“X”键，挂起 R2 的会话，返回到 R1 的控制台界面。

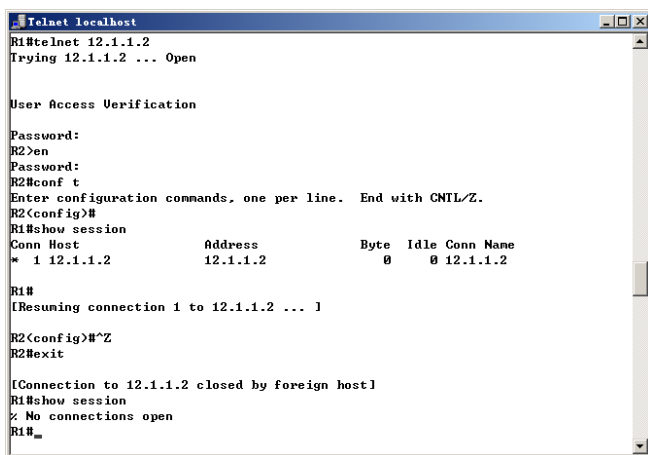


图 4-3-10 使用远程登录

- 第 11 行，在路由器 R1 上执行“show session”命令，查看路由器 R1 上打开的会话，可以看到有一个会话的编号是 1；如果打开多个连接，这里会列出多个编号，最后退出的编号前面会出现一个星号。
- 第 14 行，按回车键可以返回到最后一个连接设备，输入“show session”命令中列出的编号也可以返回到对应的连接设备。
- 第 15 行，在 R1 上按回车键，提示重新连接会话 1，连接到 12.1.1.2。
- 第 16 行，R1 重新连接到 R2，并返回到之前退出时的界面。
- 第 17 行，退出路由器 R2 的连接。exit 命令是退出，不再是挂起。
- 第 18 行，提示到路由器 R2 的连接被关闭。
- 第 19 行，再次查看打开的会话。
- 第 20 行，路由器 R1 上没有打开的会话了。也可以在 R1 的特权模式下使用“disconnect 会话号”，断开一个连接。

(4) 继续测试，在 R1 上再次登录 R2。

在 R2 上使用“show user”命令查看当前连接到路由器上的用户，图 4-3-11 显示当前有两个用户登录，编号 0 的是 Console 端口用户，编号 2 的是 VTY 0 用户。其中，编号 0 前面有一个星号，表示当前的用户是 Console 端口用户。可以使用“clear line vty 0”（相对编号）命令或“clear line 2”（绝对编号）命令来断开远程登录的用户。再次使用“show user”命令，可以发现 VTY 0 用户已经被断开。

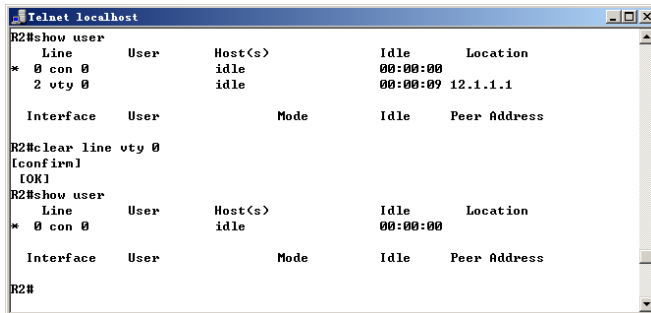


图 4-3-11 查看和断开登录的用户

(5) 限制 VTY 登录。出于安全考虑，可以限制 IP 对路由器的远程访问。配置如下：

```
R2(config)#access-list 1 permit 12.1.1.1
R2(config)#line vty 0 4
R2(config-line)#access-class 1 in
```

有关访问控制列表，本书后面有专门的章节介绍。这里读者要掌握的是，可以在 VTY 线路上挂接访问控制列表，使用的命令是 `access-class`。这样就实现了只有 12.1.1.1 可以远程访问路由器 R2。读者可以更换路由器 R1 接口 S1/1 的 IP 地址，来测试效果。

注意：当远程登录路由器时，默认设置不使用监控，无法看到从控制台直接登录时的提示消息，也无法看到一些错误输出，需要使用“`Router#terminal monitor`”命令打开 VTY 的终端监控。

7. 配置主机名列表

在 Windows 操作系统的计算机上有一个 `hosts` 文件用来定义主机名和 IP 地址的对应关系，在思科路由器上可以使用“`ip host`”命令创建主机名列表，如下所示：

```
R1(config)#ip host abc 12.1.1.2
```

配置完主机名后，路由器 R1 对 R2 的访问可以使用“`telnet abc`”，用名字取代 IP 地址。可以使用“`show host`”命令查看路由器上配置的主机名列表。

8. 配置使用 DNS 服务器

如果网络规模很大，配置主机名列表就显得难以胜任，此时就需要配置 DNS 服务器。就像现在计算机对互联网的访问一样，不是使用 `host` 主机名列表，而是使用 DNS 服务器。在路由器上配置 DNS 服务器的命令是“`ip name-server` 服务器的 IP 地址”。在图 4-3-12 中，“`ip name-server 218.2.135.1`”配置使用 DNS 服务器，要保证路由器已经可以访问 DNS 服务器 218.2.135.1 的前提下，接下来输入域名“`cbl.njut.edu.cn`”，路由器尝试使用 DNS 服务器对域名进行解析，从图中可以看出解析出的 IP 地址是 202.119.248.16，然后路由器尝试登录（Telnet）这个 IP 地址，因远程服务器没有开通 Telnet 服务，登录失败。

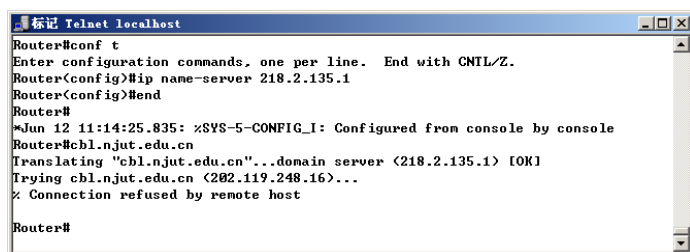


图 4-3-12 配置 DNS 服务器

路由器上往往没有必要进行域名解析，尤其是初学者很容易输错命令，当初学者输错命令后，因为路由器上没有配置 DNS 服务器，路由器将向全网（255.255.255.255）广播，查询主机名，并尝试 Telnet 登录。在图 4-3-13 中，用户输入“`conf t`”时，不小心少输入了一个空格，路由器向全网广播查找主机“`conf t`”，结果查了很久，返回失败信息。在不使用 DNS 服务器的情况下，可以关闭域名解析服务，在全局配置模式下使用“`no ip domain lookup`”命令，关闭域名查找，以后再输错命令时，路由器不再广播查找主机名，很快就可以返回结果了。关闭域名查找，并不影响配置的主机名列表，配置的主机名仍可以使用。

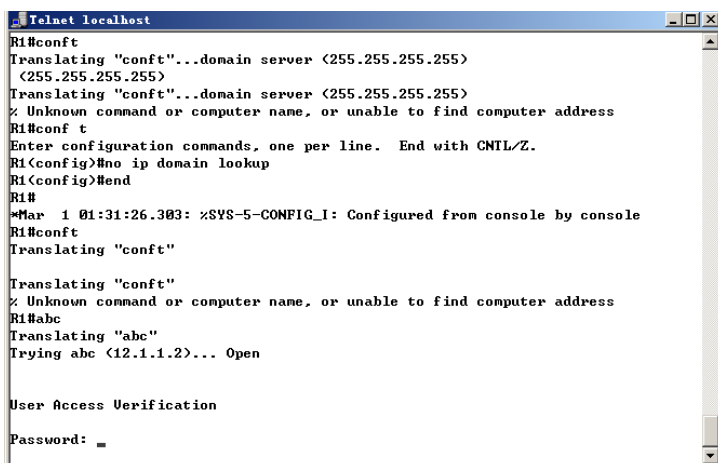


图 4-3-13 关闭域名解析服务



4.4 简单网络的配置、管理和排错**

本节结合图 4-4-1 讲解网络的配置，并演示 ping、tracert、show 和 debug 命令的使用。

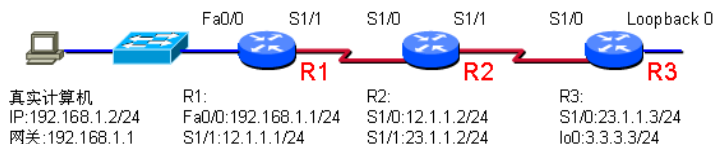


图 4-4-1 简单网络拓扑

4.4.1 配置和排错**

再次强调，本书如无特别说明，使用的模拟软件都是 Dynamips，使用 Packet Tracer 的地方都会特别说明。

1. 简单配置

根据图 4-4-1 中的拓扑，更改真实计算机的 IP 地址为 192.168.1.2，掩码为 255.255.255.0，网关为 192.168.1.1。路由器 R1 的配置如下：

```

Router>en
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut

```

路由器 R2 的配置如下：

```

Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0

```

```
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
```

路由器 R3 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#int loopback ?    查看路由器上支持的环回接口数量, 大得惊人。
<0-2147483647> Loopback interface number
```

```
R3(config)#int loopback 0
```

配置路由器 R3 的环回接口, 环回接口是一个虚拟接口, 一般用来模拟路由条目。另外, 环回接口比较稳定, 除非路由器掉电或关闭环回接口, 否则环回接口一直有效。

```
R3(config-if)#ip add 3.3.3.3 255.255.255.0
```

环回接口是一个虚拟接口, 默认是打开的, 当然再输一遍 no shut 也没有关系。

2. 测试连通性

(1) 测试网关。在真实计算机上测试到网关的连通性, 如图 4-4-2 所示。在真实计算机上执行“ping 192.168.1.1”, 结果收到了 192.168.1.1 的应答包: “Reply from 192.168.1.1: bytes=32 time=12ms TTL=255”, 其中“byte=32”表示 ping 包使用的字节数, 默认大小是 32 字节; “time=12ms”表示从发出 ping 包到收到应答, 花费的时间等于 12 毫秒, 这个值可以用来简单地判断网络的健康状况; “TTL=255”, 每经过一台路由器, TTL(Time To Live, 生存时间)这个值至少减 1, 当这个值减到零时, 路由器丢弃这个数据包。TTL 的初始值与具体的操作系统有关, 不同的操作系统默认的初始值不同, 可能的初始值是 64、128、255。假如 TTL 的值是 255, 则表示没有经过任何一台路由器就到达目标了; 假如 TTL 的值是 62, 可以判断操作系统的初始值是 64, 经过了两台路由器, 为何不会是 128-62=66 台呢? 因为现在 Internet 上任何两台主机之间的路由器都没有达到这个数值。

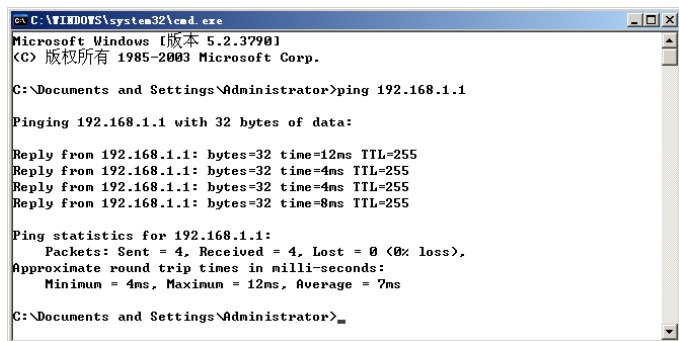


图 4-4-2 计算机上的 ping 测试

计算机上的 ping 命令, 默认发送 4 个包, 如果希望发送多个 ping 包, 可以使用“n”参数, 比如打算 ping 100 个包, 则命令是:

```
Ping 192.168.1.1 -n 100
```

如果希望持续不断地 ping, 可以使用“t”参数, 命令是:

```
Ping 192.168.1.1 -t
```

使用带“t”参数的 ping，计算机持续不断地发送 ping 包，可以使用“Ctrl + C”组合键终止命令的执行。

如果 ping 网关失败，就要检查物理线路是否正常，如果物理链路正常，接下来 ping 127.0.0.1，看计算机上的 TCP/IP 协议栈是否正常，如果也正常，再 ping 本计算机的 IP 地址，来检查网卡的驱动程序安装是否正常，再接下来检查计算机的子网掩码是否正常，有没有使用防火墙等，一般排除网络故障的步骤是从低层向高层、逐层排查的。

(2) 测试不同子网的 IP 地址。在真实计算机上 ping 路由器 R1 S1/1 接口的 IP 地址“12.1.1.1”，结果显示可以 ping 通，继续在真实计算机上 ping 路由器 R2 S1/0 接口的 IP 地址“12.1.1.2”，结果收到“Request timed out.”信息，提示 ping 超时，也就是网络不通，造成网络不通的原因是什么呢？会不会是因为真实计算机的 ping 包没有到达路由器 R2 呢？在路由器 R2 上执行 debug 命令进行调试，同时在真实计算机上继续 ping 路由器 R2 S1/0 接口的 IP 地址，路由器 R2 的显示如下：

```
R2#debug ip icmp ping 使用的是 ICMP 协议，debug 是一个调试命令，主要用来排查网络故障。使用
undebug all 命令关闭所有 debug。
ICMP packet debugging is on
R2#
*Jun 12 19:10:44.642: ICMP: echo reply sent, src 12.1.1.2, dst 192.168.1.2
*Jun 12 19:10:49.930: ICMP: echo reply sent, src 12.1.1.2, dst 192.168.1.2
*Jun 12 19:10:55.438: ICMP: echo reply sent, src 12.1.1.2, dst 192.168.1.2
*Jun 12 19:11:00.914: ICMP: echo reply sent, src 12.1.1.2, dst 192.168.1.2
R2#
```

从上面的输出中可以看到，路由器 R2 已经收到来自真实计算机“192.168.1.2”的 ping 包，即 echo request 包，并且发送了 echo reply 应答包。我们知道网络通信是双向的，真实计算机的 ping 包到达路由器 R2，并能从路由器 R2 收到应答包才表示网络连通。从上面的 debug 消息中可以看到，路由器 R2 已经收到了真实计算机发过来的 ping 包，并且也发送了应答包。应答包有没有被发送出去呢？在路由器 R2 上执行“show ip route”命令，查看路由器 R2 的路由表，显示如下：

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    23.0.0.0/24 is subnetted, 1 subnets
C       23.1.1.0 is directly connected, Serial1/1
    12.0.0.0/24 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, Serial1/0
R2#
```

命令输出的前半部分是固定不变的，“C”表示的是直连路由，“S”表示的是静态路由，“R”表示的是 RIP（Routing Information Protocol，路由信息协议，动态路由中的一种，本书第 6 章专门介绍该协议）路由，“D”表示的是 EIGRP（Enhanced Interior Gateway Routing Protocol，增强内部网关路由协议，也是动态路由协议中的一种，本书第 7 章专门介绍该协议）路由，“O”表示的是 OSPF（Open Shortest-Path First，开放式最短路径优先，也是动态路由协议中的一种，本书第 8 章专门介绍该协议）路由，“*”表示的是默认路由（有时也称

缺省路由)，CCNA 中只会涉及这些路由，后面章节会详细介绍每一种路由。从上面的输出中可以看出，路由器 R2 的路由表中有两条直连路由，至于每个条目为何显示成两行，本书“6.5.1 路由表结构”一节会详细介绍，去往 23.1.1.0/24 的数据包从 Serial1/1 口发出，去往 12.1.1.0/24 的数据包从 Serial1/0 口发出。去往 192.168.1.2 的数据包往哪里发出呢？R2 的路由表中没有去往 192.168.1.2 的路由，R2 丢弃去往 192.168.1.2 的数据包。

使用下面的命令在路由器 R2 上添加去往 192.168.1.2 的路由，命令如下：

```
R2(config)#ip route 192.168.1.0 255.255.255.0 12.1.1.1
```

这里添加的是静态路由，先不对命令进行解释，本书“5.3 静态路由”一节会详细介绍。在真实计算机上再次 ping 12.1.1.2，结果显示能够 ping 通了。

3. 添加路由

使用下面的命令在 R1、R2、R3 上添加路由，本章不对添加路由的命令进行解释，这里仅完成网络的连通，下一章再解释静态路由的配置命令。

R1 的配置如下：

```
R1(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.2
```

R2 的配置如下：

```
R2(config)#ip route 192.168.1.0 255.255.255.0 12.1.1.1  
R2(config)#ip route 3.3.3.0 255.255.255.0 23.1.1.3
```

R3 的配置如下：

```
R3(config)#ip route 0.0.0.0 0.0.0.0 23.1.1.2
```

4. 进一步测试网络的连通性

在路由器 R1 上 ping 路由器 R3 的 3.3.3.3，结果显示如下：

```
R1#ping 3.3.3.3  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/36/64 ms  
R1#
```

路由器默认发送 5 个 ping 包，收到应答时显示“！”。在路由器 R3 上使用下面的命令关闭 loopback 0：

```
R3(config)#int lo0  
R3(config-if)#shut
```

在路由器 R1 上再次 ping 路由器 R3 的 3.3.3.3，结果显示是“.....”，“.”表示超时。造成超时的原因是因为这里产生了路由的环路，本书下一章的“5.4 默认路由”一节将对路由环路问题进行深入讨论。

打开路由器 R3 的 loopback 0，关闭路由器 R2 的 S1/1 接口，在路由器 R1 上再次 ping 路由器 R3 的 3.3.3.3，结果显示如下：

```
R1#ping 3.3.3.3  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:  
U.U.U  
Success rate is 0 percent (0/5)  
R1#
```

“U”的意思是数据包不可达，路由器 R1 把数据包发给路由器 R2，R2 查询本地的路由表，发现没有去往 3.3.3.3 的路由，路由器 R2 发送主机不可达的消息告诉路由器 R1，目标主机不可达，路由器 R1 上显示“U”标记。有关这一点，可以在路由器 R1 上使用“debug ip icmp”命令，打开 ICMP 消息监控，再次在 R1 上 ping 3.3.3.3，路由器 R1 的 debug 输出如下：

```
*Mar 1 05:21:18.754: ICMP: dst (12.1.1.1) host unreachable rcv from 12.1.1.2
```

使用“show ip route”命令查看路由器 R2 的路由表，显示如下：

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    12.0.0.0/24 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, Serial1/0
S       192.168.1.0/24 [1/0] via 12.1.1.1
```

从上面的输出中可以看到关闭路由器的 S1/1 接口，丢失了该接口的直连路由和去往 3.3.3.3 的静态路由。

5. 高级 ping 命令

在计算机上可以使用带参数的 ping 命令来执行一些特殊的功能，在路由器上也可以使用高级的 ping 命令来扩展 ping 的功能。在路由器 R1 上，高级的 ping 命令执行如下：

```
R1#ping                               输入 ping 直接回车，使用高级 ping 命令。
Protocol [ip]:                         使用的是 IP 协议，直接回车。
Target IP address: 12.1.1.2           ping 的目标 IP 地址
Repeat count [5]: 20                  ping 包的个数，默认值是 5，这里输入 20。
Datagram size [100]:                  ping 包的默认大小是 100 字节
Timeout in seconds [2]:                默认超时时间是 2 秒，2 秒内收不到应答即认为超时。
Extended commands [n]: y              是否要进一步扩展 ping 命令，这里选择扩展。
Source address or interface: 192.168.1.1
ping 使用的源地址，如果这里不填，路由器将使用离目标最近的端口进行 ping，也就是使用
12.1.1.1 去 ping，这里指定的是路由器 R1 另一个接口 Fa0/0 的 IP 地址作为源地址去 ping。
Type of service [0]:                  接下来的选项，超出 CCNA 的讨论范围，都直接回车。
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 20, 100-byte ICMP Echos to 12.1.1.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (20/20), round-trip min/avg/max = 12/23/48 ms
R1#
```

6. traceroute 命令

ping 命令可以用来测试网络的连通性，如果网络不通，ping 命令无法定位到问题出在哪一台中间设备上，此时可以使用 traceroute 命令来测试中间经过哪些设备、问题出在哪里等。在路由器 R1 上执行“traceroute 23.1.1.3”命令，结果如图 4-4-3 上半部分所示，可以发

现问题出在路由器 12.1.1.2 上，此时下面一段在计算机上的测试也同时进行。打开路由器 R2 的 S1/1 口，再次执行“tracert 23.1.1.3”命令，结果如图 4-4-3 下半部分所示，提示要到达 23.1.1.3，首先经过 12.1.1.2。

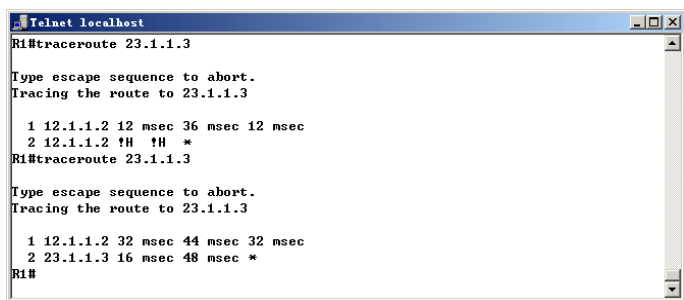


图 4-4-3 路由器上 traceroute 测试

tracert 采用的工作原理是：发送设备将数据包中的 TTL 设成 1，数据包会被第一跳路由器丢弃，返回一个错误码信息，源设备据此判断经过的中间设备和延时信息，源设备一般发送 3 个重复的包，在图 4-4-3 中，可以看到 3 个返回时间“1 12.1.1.2 12 msec 36 msec 12 msec”；源设备接着发送 TTL 为 2 的数据包，再发送 TTL 为 3 的数据包，直至到达目标设备或 TTL 到达 30 为止。在正常情况下，TTL 不会超过 30 就可以到达目标设备，除非存在路由环路的情况下，TTL 才会增加到 30。

在真实计算机上执行“tracert 23.1.1.3 -d”命令，结果如图 4-4-4 上半部分所示，可以发现问题出在路由器 12.1.1.2 上。打开路由器 R2 的 S1/1 口，再次执行“tracert 23.1.1.3 -d”命令，结果如图 4-4-4 下半部分所示，提示要到达 23.1.1.3，首先经过 192.168.1.1，然后经过 12.1.1.2，最终到达目的地。tracert 命令试图把所有 IP 地址解析成域名，这个过程很耗时间，往往也没有意义，使用“-d”参数的作用是不执行反向解析，这样执行的速度会大大加快。

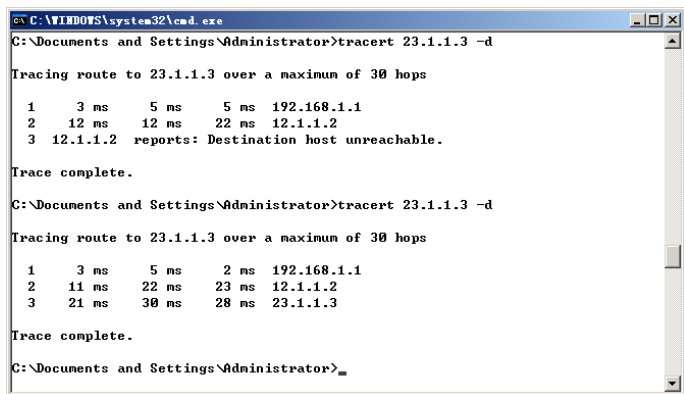


图 4-4-4 计算机上 tracert 测试

注意：在路由器上是 traceroute，命令可以简写成“tr”；在计算机上是 tracert，命令不可简写。在路由器上输入“tracer”是正确的，但如果输入“tracert”就是错误的了。

7. 常用排错命令

除了前面使用到的一些命令外，下面这些命令对排错也很有帮助。

“show interface”命令用来查看路由器的接口状态，在路由器 R1 上使用“show interface”命令，部分结果显示如下：

```
R1#show interface
执行 show interface 命令会显示路由器所有接口的信息，如果只想查看某一个接口的情况，可以使用 “show
interface + 具体的接口” 命令，比如 show int fa 0/0，将只显示 fastethernet0/0 接口的信息。
FastEthernet0/0 is up, line protocol is up 接口是 UP 的，协议也是 UP 的，这表示接口正常。
Hardware is AmdFE, address is cc07.0a70.0000 (bia cc07.0a70.0000)
接口是快速以太网，接口的 MAC 地址是 cc07.0a70.0000。
Internet address is 192.168.1.1/24 接口的 IP 地址和子网掩码。
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, 接口的 MTU (Max Transport Unit, 最大
传输单元) 是 1500 字节，带宽是 100Mbps，延时 100 微秒。
省略部分输出。
Serial1/0 is administratively down, line protocol is down
administratively down 表示管理 Down，也就是没有被管理员使用 no shutdown 命令打开的端口；如果
端口和协议都是 Down 的，多数是硬件有问题；如果端口是 UP 的，协议是 Down 的，可能是端口没有接线，或
对端设备没有打开这个端口。对于串行接口，还可能是两边协议封装得不一致，或时钟没有设置等；端口和协
议都是 UP 表示端口工作正常；端口 Down、协议 UP 的情况不可能存在。
省略部分输出。
Serial1/1 is up, line protocol is up 端口工作正常。
Hardware is M4T 端口的硬件模块类型。
Internet address is 12.1.1.1/24 IP 地址和子网掩码。
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, 带宽是 1.544Mbps。
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, crc 16, loopback not set
封装的协议是 HDLC，广域网部分还会介绍其他的封装协议。
省略部分输出。
```

“show ip interface”命令用来查看接口与 IP 相关的信息，R1 上的部分输出如下：

```
R1#show ip interface fa 0/0 仅查看 fastethernet 接口的情况。
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set 没有启用 DHCP 的辅助寻址，在 DHCP 部分
会使用到 ip helper address 命令。
Directed broadcast forwarding is disabled
Outgoing access list is not set
接口外出方向没有使用访问控制列表，在 ACL 一章，可以使用这个命令来验证接口下有没有使用 ACL。
Inbound access list is not set 接口进入方向没有使用访问控制列表。
Proxy ARP is enabled
代理 ARP 启用，可以在接口下使用 no ip proxy-arp 禁用代理 ARP 功能，有关代理 ARP，本书
2.4.2 节已经介绍过，5.3 节会演示如何使用代理 ARP。
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled 水平分隔是启用的，一些动态路由协议，比如 RIP 与水平分隔的关系很大。
省略部分输出。
```

“show ip interface”命令显示的项目很多，更常用的是查看接口状态，使用的命令是“show ip interface brief”。从下面的输出中可以看到，Fa0/0 和 S1/1 接口工作正常，其他几个端口都没有打开。

```
R1#show ip int brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 192.168.1.1 YES manual up up
Serial1/0 unassigned YES unset administratively down down
Serial1/1 12.1.1.1 YES manual up up
Serial1/2 unassigned YES unset administratively down down
Serial1/3 unassigned YES unset administratively down down
FastEthernet2/0 unassigned YES unset administratively down down
```

R1#

“show arp”命令用来查看路由器的 ARP 表，相当于计算机上的“arp -a”命令。可以使用“clear arp”命令清除 ARP 缓存，相当于计算机上的“arp -d”命令。“show arp”命令执行如下：

```
R1#show arp
Protocol Address      Age (min) Hardware Addr  Type   Interface
Internet 192.168.1.1        -    cc07.0a70.0000  ARPA    FastEthernet0/0
Internet 192.168.1.2        0    001b.247d.2572  ARPA    FastEthernet0/0
R1#
```

“show controllers”命令用来查看接口的硬件信息，也可以用来查看接口连接线缆的类型。下面是在模拟路由器 R1 上执行的结果。

```
Router#show controllers s1/1
M4T: show controller:
PAS unit 1, subunit 1, f/w version 1-45, rev ID 0x2800001, version 1
idb = 0x640C7C34, ds = 0x640C8CFC, ssb=0x640C90B8
Clock mux=0x0, ucmd_ctrl=0x0, port_status=0x7B
Serial config=0x8, line config=0x200
maxdgram=1608, bufpool=78Kb, 120 particles
DCD=up DSR=up DTR=up RTS=up CTS=up
line state: down
cable type : V.11 (X.21) DCE cable, received clockrate 2015232
使用的线缆是 V.11，本接口连接的是 DCE 端。
省略部分输出。
```

在 Packet Tracer 中，打开 First.pkt 拓扑，在路由器 Router0 和 Router1 上使用“show controller s0/0/0”命令查看。Router0 的显示如下：

```
Router#show controllers s0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, no clock
使用的线缆是 V.35，本接口连接的是 DCE 端。
```

Router1 的显示如下：

```
Router#show controllers s0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DTE V.35, no clock
使用的线缆是 V.35，本接口连接的是 DTE 端。
```

4.4.2 文件管理***

路由器上的文件包括：IOS、运行配置文件（running-config）、启动配置文件（startup-config）。有关 IOS 文件的备份、升级和恢复请参考本书 18.4.1 节。本节仅介绍运行配置文件和启动配置文件的管理。

1. 运行配置文件管理

(1) 查看运行配置文件。使用“show running-config”命令查看运行配置文件，使用“show startup-config”命令查看保存的配置文件。“show running-config”命令的执行如下：

```
Router#show run
Building configuration...

Current configuration : 846 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```

!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface Serial1/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
interface FastEthernet2/0
--More--

```

一屏显示不完，下面会出现“--More--”的提示，按回车键下翻一行，按空格键下翻一屏，按其他任意键退出。

(2) 新建配置文件。对路由器的配置可以一行一行地输入，也可以先用文本编辑器编辑，然后直接粘贴到路由器的控制台，比如输入下列的文本内容：

```

En
Conf t
Host R1
Int fa 0/0
Ip add 192.168.1.1 255.255.255.0
No shut

```

事实上，很多经验丰富的工程师都使用这种配置方式来节省配置时间。

(3) 保存运行配置文件。当前起作用的配置是运行配置文件，如果不保存运行配置文件，路由器重启后，以前的运行配置文件将丢失。如果路由器中有启动配置文件，启动配置文件将被拷贝到内存中，成为运行配置文件；如果路由器中没有启动配置文件，路由器将提示是否进入 **Setup** 模式。可以使用下面的命令保存路由器的运行配置文件：

```
R1#copy running-config startup-config
```

一般简写成 `copy run start`，用运行配置文件覆盖启动配置文件。

或者

R1#write

一般简写成 wr，用运行配置文件覆盖启动配置文件。

(4) 拷贝运行配置文件到 TFTP 服务器。

在真实计算机上解压缩 CCNANEW.rar 文件中的 tftpsvr.rar 文件，双击 tftpsvr.exe 文件，开始安装思科的 TFTP 服务器软件。双击桌面上的“Cisco TFTP Server”快捷图标，启动 TFTP 服务。路由器 R1 的执行如下：

```
R1#copy startup-config tftp
Address or name of remote host []? 192.168.1.2    输入 TFTP 服务器的 IP 地址。
Destination filename [r1-config]?                拷贝到 TFTP 服务器上的文件名。
!!                                                拷贝过程。
954 bytes copied in 0.216 secs (4417 bytes/sec)    拷贝成功。
R1#
```

Cisco TFTP Server 上显示从 192.168.1.1 上成功接收到文件“r1-config”。单击菜单“View”→“Options”，打开如图 4-4-5 所示的 Options 窗口，可以看到 TFTP server 的默认根路径为“C:\Program Files\Cisco Systems\Cisco TFTP Server”，这个默认路径可以更改。

在这个文件夹下，找到 r1-config 文件，可以使用 Windows 自带的“记事本”或“写字板”程序打开，如图 4-4-6 所示。可以对这个文件进行编辑，然后通过 TFTP 的方式再回传到路由器上，保存的时候要注意，使用纯文本的格式。也可以全部复制，然后进入路由器的特权配置模式下，把文本文件粘贴进来。

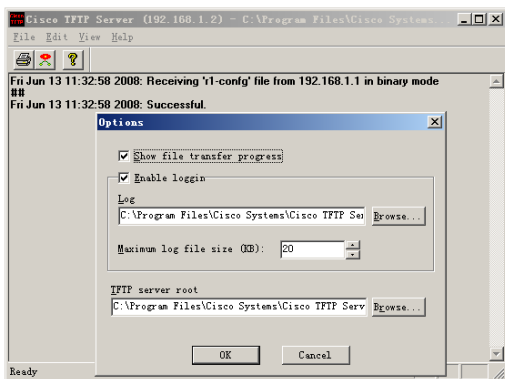


图 4-4-5 TFTP 服务

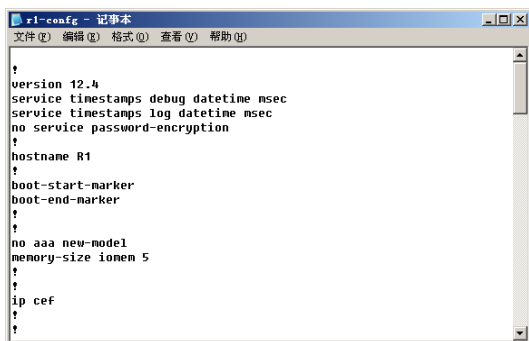


图 4-4-6 查看配置文件

(5) 恢复运行配置文件。可以使用下面的命令恢复配置文件：

```
R1#copy startup-config running-config
```

这里要特别提醒的是，把备份的配置文件拷贝到运行的配置文件上，使用的不是覆盖，而是合并。比如运行配置文件的接口是 shutdown 的，启动配置文件中没有 shutdown 命令，隐含是打开的，拷贝完成后，两个文件进行合并，结果是 shutdown 仍然存在，接口保持关闭。有关这一点要特别注意。

或者从 TFTP 服务器恢复配置：

```
R1#copy tftp running-config
Address or name of remote host []? 192.168.1.2
Source filename []? r1-config
Destination filename [running-config]?
```

2. 启动配置文件管理

(1) 备份和恢复启动配置文件。为了安全起见，也可以使用 TFTP 的方式对启动配置文件进行备份和恢复，使用的命令如下：

```
R1#copy startup-config tftp    把启动配置文件拷贝到 TFTP 服务器上。
```

```
R1#copy tftp startup-config
```

从 TFTP 服务器上恢复启动配置文件。

(2) 删除启动配置文件。使用下面的命令删除启动配置文件：

```
R1#erase startup-config
```

要取消对路由器的某行配置，一般是在对应的行前加 **no**。

3. 捕获文字

这里介绍一种使用“超级终端”捕获文字录入过程的方法，这种方法一般用在考试的环境中，比如国内锐捷的认证考试就要求捕获文字的录入过程。这里以捕获路由器 R1 控制台的输入为例，操作如下：

① 设置超级终端连接参数。单击“开始”→“程序”→“附件”→“通信”→“超级终端”，打开“连接描述”对话框，随便输入一个名字，接下来询问连接到哪里，如图 4-4-7 所示。在“连接时使用”中选择“TCP/IP (Winsock)”，在“主机地址”中填入计算机的 IP 地址“192.168.1.2”，在“端口号”中填入“3008”，端口号可以在图 4-1-20 中查看到。

② 开始捕获文字。单击菜单“传送”→“捕获文字”，打开“捕获文字”设置对话框，在文件栏中填入捕获文字保存的文件名和路径。

③ 停止捕获。单击菜单“传送”→“捕获文字”→“停止”，停止捕获文字，如图 4-4-8 所示。

④ 查看捕获的文字。找到对应的文件，进行查看。也可使用“show running-config”或“show startup-config”命令，然后对文本文件编辑一下，删除多余的行，得到所需的配置。

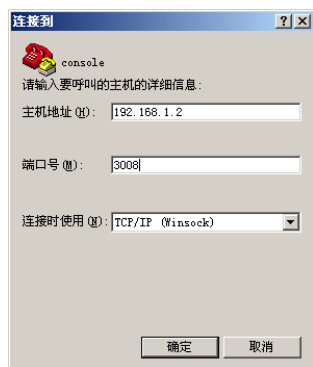


图 4-4-7 超级终端连接

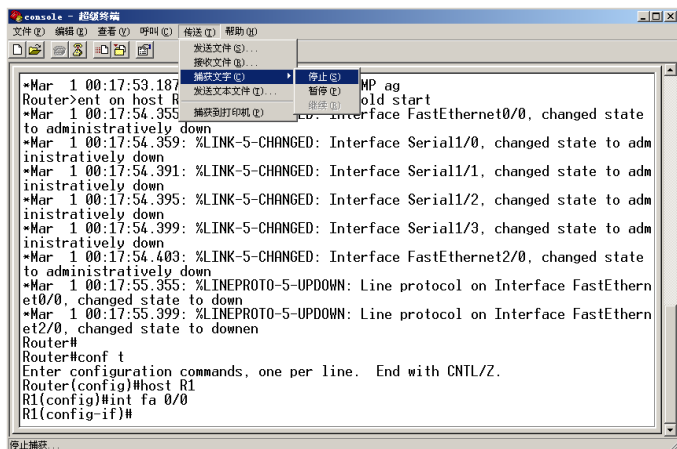


图 4-4-8 停止捕获文字



4.5 CDP 协议**

CDP (Cisco Discovery Protocol, 思科发现协议) 是思科公司的专用协议，有助于网络管理员收集本地和远程连接设备的相关信息。可用于发现和绘制网络连接拓扑，帮助排除网络故障。

4.5.1 CDP 介绍**

CDP 协议工作在 OSI 七层模型的第二层 (即数据链路层)，也就是说，只要物理层和数

据链路层正常，CDP 就可以正常工作，和高层的网络层没有关系。CDP 是思科公司私有的协议，也就是说，该协议并不能用于其他的非思科公司的设备。

网络管理员把 CDP 作为信息收集工具，来获知直接相连的思科设备的信息。在默认情况下，思科设备启用 CDP 协议，并周期性地发送 CDP 通告给直接相连的思科设备，通告中会包括连接设备的类型（比如是路由器还是交换机）、相关的接口、设备的型号（比如是 1841 还是 7200）。

4.5.2 CDP 应用**

接下来结合应用讲解 CDP 协议，开启 CCNA 模拟机架中的 SW1、R1、R2，使用 CDP 协议来发现它们之间的连接。

这里假设不知道它们之间是如何连接的，因为 CDP 协议是第二层的协议，为了使 CDP 协议能够正常工作，开启所有设备的所有接口。SW1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host SW1
```

这里值得提醒的是，SW1 上的所有接口都是交换模块上的接口，对于交换机来说，二层接口默认都是打开的，如果不放心也可以使用下面的命令打开所有的接口。

```
SW1(config)#int range fa 1/0 - 15
SW1(config-if-range)#no shut
```

对于交换机，可以一次配置多个接口，范围从 fa 1/0 到 fa 1/15，共 16 个接口。

在路由器 R1 上使用“show ip int brief”命令，查看路由器 R1 上总共有哪些接口，依次使用 no shut 打开所有的接口，配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0
R1(config-if)#no shut
R1(config-if)#int fa 2/0
R1(config-if)#no shut
R1(config-if)#int s1/0
R1(config-if)#no shut
R1(config-if)#int s1/1
R1(config-if)#no shut
R1(config-if)#int s1/2
R1(config-if)#no shut
R1(config-if)#int s1/3
R1(config-if)#no shut
```

如果在一些低端的老式设备上，还要注意配置串行接口 DCE 端的时钟，可以使用“show controllers”命令查看串行接口上的线缆是不是 DCE 端，或者不管是 DCE 还是 DTE 都在接口下配置 clock rate 64000，DTE 端会报错，配置时钟失败，但不影响执行；DCE 配置成功。在 Dynamips 模拟器上可以省掉这个命令了，在 Packet Tracer 模拟器中不能省略，如果使用的是 First.pkt 拓扑，需要在路由器 Router0 的 S0/0/0 接口配置时钟。路由器 R2 的配置与 R1 类似，也是打开所有端口。

使用“show cdp”命令查看 CDP 的全局信息，包括：发送 CDP 的时间间隔，默认是 60 秒；CDP 的保持时间，默认是 180 秒；CDP 协议的版本，当前默认使用的是 CDPv2。SW1、R1、R2 的显示结果相同，其中 SW1 的显示如下：

```
SW1#show cdp
Global CDP information:
```

```
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled
```

可以使用下面的命令更改 CDP 的发送间隔和保持时间，配置如下：

```
SW1(config)#cdp timer 10          CDP 发送时间间隔是 10 秒。
SW1(config)#cdp holdtime 40       CDP 保持时间是 40 秒。
```

可以使用“show cdp”命令验证结果，使用下面的命令关闭 CDP 协议：

```
SW1(config)#no cdp run           关闭 CDP 协议。
SW1(config)#do show cdp
show 命令的执行模式是在特权模式下，新版本的 IOS 中新增了一个特权命令 do 的使用，可以在其他模式下调用特权命令，使用带 do 的命令，而不需要退回到特权模式下，直接执行命令。Packet Tracer 模拟器不支持 do 命令。
% CDP is not enabled             提示 CDP 没有运行。
SW1(config)#
```

验证完成后，使用“cdp run”命令使 SW1 恢复运行 CDP 协议。

! 注意：使用 Dynamips 模拟器时，会频繁地看到类似下面的提示：

“*Mar 1 00:35:24.811: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet1/6 (not half duplex), with R1 FastEthernet2/0 (half duplex).”

CDP 协议报告双工不匹配的提示，在不使用 CDP 协议的情况下，可以使用“no cdp run”命令关闭 CDP 协议，这样的提示信息就不会再出现了。本书后面的各章都关闭 CDP 协议。

使用“show cdp interface”命令验证哪些接口运行了 CDP 协议，在默认情况下，思科设备的所有接口都运行 CDP 协议。可以在接口下使用“no cdp enable”命令关闭某个接口的 CDP 协议。路由器 R1 上的配置和校验如下：

```
R1(config)#int s1/1
R1(config-if)#no cdp enable       关闭 S1/1 的 CDP 协议。
R1(config-if)#int s1/2
R1(config-if)#no cdp enable       关闭 S1/2 的 CDP 协议。
R1(config-if)#int fa0/0
R1(config-if)#no cdp enable       关闭 Fa 0/0 的 CDP 协议。
R1(config-if)#do show cdp interface 验证运行 CDP 协议的接口。
Serial1/0 is up, line protocol is down
Encapsulation HDLC
接口封装的是 HDLC 协议，默认运行 CDP 协议，CDP 协议发送的时间间隔是 60 秒，保持时间是 180 秒。这里要提醒的是，如果接口封装的是帧中继，默认是禁用 CDP 协议的，但可以使用“cdp enable”命令启用 CDP 协议。
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Serial1/3 is up, line protocol is down
Encapsulation HDLC
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
FastEthernet2/0 is up, line protocol is up
Encapsulation ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
R1(config-if)#
```

从上面的输出中可以看出，路由器 R1 上除 S1/1、S1/2、Fa0/0 接口外，所有的接口都运行了 CDP 协议，这里使用“cdp enable”命令恢复 S1/1、S1/2、Fa0/0 接口的 CDP 协议。

使用“show cdp neighbors”命令收集邻居信息。其中 R1 上执行结果如下：

```
R1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater
```


Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
C6509	Fas 0/0	149	R S	WS-C6509	Gig 9/36
SW1	Fas 2/0	33	R S I	3640	Fas 1/6
R2	Ser 1/1	126	R	7206VXR	Ser 1/0
R2	Fas 0/0	175	R	7206VXR	Fas 2/0
R2	Fas 0/0	173	R	7206VXR	Fas 0/0
R1#					

路由器 R1 上的 CDP 邻居信息解释如表 4-5-1 所示。

表 4-5-1 CDP 邻居信息表

字 段	解 释
Device ID	邻居设备的 hostname
Local Intrfce	表示当前设备的本地接口
Holdtme	表示保持时间，比如，C6509 的保持时间是 149 秒，也就是说，再过 149 秒，这个邻居设备消失，事实上这个邻居设备不会消失，因为发送 CDP 的时间间隔默认是 60 秒，149 秒表示收到上一个 CDP 包已经有 180-149=31 秒了，再过 29 秒将收到下一个 CDP 包，这个值正常不会少于 120。为何 SW1 的保持时间是 33 秒内，因为之前将 SW1 的发送时间间隔调成了 10 秒，保持时间调成了 40 秒，在正常情况下，SW1 的保持时间不会小于 30
Capability	表示连接的设备，“R”表示路由器，“S”表示交换机，“R S”则表示路由交换机
Platform	表示设备的具体型号，如 3640、WS-C6509、7206VXR 等
Port ID	表示远端设备的连接接口

从上面的输出中，读者可能会奇怪路由器 R1 的 Fa0/0 接口怎么能同时连接 C6509（笔者的笔记本电脑连接在单位的思科 6509 交换机的 Gi 9/36 接口）的 Gi 9/36 接口、R2 的 Fa2/0 接口、R2 的 Fa0/0 接口。原因是 R1 的 Fa0/0、R2 的 Fa2/0、R2 的 Fa0/0、C6509 的 Gi9/36 都连接在 SW4 上，这里的 SW4 是一台交换机，但不是思科公司的交换机（如果真是思科公司的交换机，将在邻居表中以“S”显示出来），也不是思科公司的集线器（如果真是思科公司的集线器，将在邻居表中以“r”显示出来），SW4 对 CDP 协议来讲，相当于一个透明的设备。事实上，笔者在思科设备的中间串接其他厂家的交换机或集线器，CDP 协议工作完全正常，也就是说，CDP 协议可以透明穿越其他公司的交换机或集线器。可以得出结论是，思科设备中间串接非思科的交换机或集线器，不影响 CDP 协议的使用。

根据上面路由器 R1 上 CDP 显示的邻居信息可以画出如图 4-5-1 所示的拓扑图，与 CCNA 机架拓扑一致，并且还有额外的发现，即发现真实计算机是接在思科 6509 的 Gi9/36 接口上的。

使用“show cdp neighbors detail”命令显示连接到此设备的邻居设备的详细信息，下面是路由器 R1 执行此命令的部分输出，比“show cdp neighbors”命令显示的信息更多，详见斜体部分的解释。

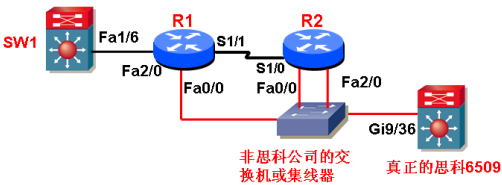


图 4-5-1 CDP 发现的拓扑

```
R1#show cdp nei detail
-----
Device ID: NJUT-6509                               邻居设备 ID。
Entry address(es):                                  地址。
  IP address: 10.0.248.1                             仅显示网段的 IP 地址。
Platform: cisco WS-C6509, Capabilities: Router Switch
硬件平台是思科 6509 的路由交换机。
```

Interface: FastEthernet0/0, Port ID (outgoing port): GigabitEthernet9/36
邻居设备的接口。

Holdtime : 159 sec 保持的时间。

Version : 下面是 IOS 版本信息。

Cisco Internetwork Operating System Software
IOS (tm) s72033 rp Software (s72033 rp-JK903SV-M), Version 12.2(18)SXD7b, RELEAS
E SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Fri 08-Dec-06 13:32 by ccai

advertisement version: 2 VTP 版本 2, 有关 VTP, 后面有专门的章节介绍。

VTP Management Domain: 'test' VTP 的域名是 test。

Native VLAN: 218 本地 VLAN 是 218。

Duplex: full

双工显示为全半双工, 因为 SW4 是一个连接共享的设备, 相当于集线器, 集线器只能工作在半双工的方式下, 可真正的交换机工作在全双工的模式下, 二者有冲突, 这就是路由器一直提示双工不一致的原因。解决这种不一致提示信息的办法是关闭 CDP 协议或者登录到真正的交换机上, 把端口设成半双工。

Device ID: SW1

Platform: Cisco 3640, Capabilities: Router Switch IGMP

Interface: FastEthernet2/0, Port ID (outgoing port): FastEthernet1/6

Holdtime : 37 sec

Version :

Cisco IOS Software, 3600 Software (C3640-IK903S-M), Version 12.4(10), RELEASE SO
FTWARE (fcl)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2006 by Cisco Systems, Inc.

Compiled Wed 16-Aug-06 04:04 by prod_rel_team

advertisement version: 2

VTP Management Domain: ''

Duplex: full

Device ID: R2

省略部分输出。

“show cdp entry *”命令和“show cdp neighbors detail”命令显示的结果相同, 可以在“show cdp entry”命令后面跟具体的邻居设备名, 如“show cdp entry SW1”命令, 仅显示某个邻居设备的信息, 注意这里的邻居设备名是区分大小写的。

“show cdp traffic”命令显示发送和接收 CDP 数据包的数量及 CDP 出错信息。该命令显示如下:

```
R1#show cdp traffic
CDP counters :
  Total packets output: 329, Input: 940
  Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
  No memory: 0, Invalid packet: 0, Fragmented: 0
  CDP version 1 advertisements output: 0, Input: 0
  CDP version 2 advertisements output: 329, Input: 940
```

“clear cdp counters”命令清除 CDP 收发数据包的计数器。“debug cdp events”命令显示 CDP 事件信息。



4.6 真题精选***

1. There are no boot system commands in a router configuration in NVRAM. What is

the fallback sequence that the router will use to find an IOS during reload?

- A. TFTP server, Flash, NVRAM
- B. ROM, NVRAM, TFTP server
- C. NVRAM, TFTP server, ROM
- D. Flash, TFTP server, ROM
- E. Flash, NVRAM, ROM

2. During startup, the router displays the following error message: boot: cannot open "flash:" What will the router do next?

- A. Because of damaged flash memory, the router will fail the POST.
- B. It will attempt to locate the IOS from a TFTP server. If this fails, it will initiate the setup dialog.
- C. It will attempt to locate the IOS from a TFTP server. If this fails, it will load a limited IOS from ROM.
- D. It will attempt to locate the configuration file from a TFTP server. If this fails, it will initiate the setup dialog.
- E. It will attempt to locate the configuration file from a TFTP server. If this fails, it will load a limited configuration from ROM.

3. A Cisco router is booting and has just completed the POST process. It is now ready to find and load an IOS image. What function does the router perform next?

- A. It checks the configuration register.
- B. It attempts to boot from a TFTP server.
- C. It loads the first image file in flash memory.
- D. It inspects the configuration file in NVRAM for boot instructions.

4. Refer to the exhibit. For what two reasons has the router loaded its IOS image from the location that is shown? (Choose two.)

```
Router1> show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-J-M), Experimental Version 11.3(19970915:164752)
[hampton-nitro-baseline 249]
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Wed 08-Oct-97 06:39 by hampton
Image text-base: 0x60008900, data-base: 0x60B98000

ROM: System Bootstrap, Version 11.1(11855) [beta 2], INTERIM SOFTWARE
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 11.1(472), RELEASE SOFTWARE (fcl)

Router1 uptime is 23 hours, 33 minutes
System restarted by abort at PC 0x6022322C at 10:50:55 PDT Tue Oct 21 1997
System image file is "tftp://172.16.1.129/hampton/nitro/c7200-j-mz"

cisco 7206 (MPE150) processor with 57344K/8192K bytes of memory.

<output omitted>

Configuration register is 0x2102
```

- A. Router1 has specific boot system commands that instruct it to load IOS from a TFTP server.
- B. Router1 is acting as a TFTP server for other routers.
- C. Router1 cannot locate a valid IOS image in flash memory.
- D. Router1 defaulted to ROMMON mode and loaded the IOS image from a TFTP server.
- E. Cisco routers will first attempt to load an image from TFTP for management purposes.

5. What is the effect of using the service password-encryption command?

- A. Only the enable password will be encrypted.

- B. Only the enable secret password will be encrypted.
 - C. Only passwords configured after the command has been entered will be encrypted.
 - D. It will encrypt the secret password and remove the enable secret password from the configuration.
 - E. It will encrypt all current and future passwords.
6. Refer to the exhibit. On an external corporate router, the network administrator enters the MOTD configuration that is shown in the upper box. The administrator then logs into the router and sees the login screen dialog that is shown in the lower box. Why does the intended message not display?

```
Router(config)# banner motd #
Enter TEXT message. End with the character '#'.
This system is the property of ABC Corporation.

For systems help, please contact our help desk at #5555. Any activity on this
system will be logged.#

Router(config)#
```

MOTD Configuration

```
Router con0 is now available

Press RETURN to get started.

This system is the property of ABC Corporation.

For systems help, please contact our help desk at

Router>
```

Login Screen Dialog

- A. The network administrator defined an illegal delimiting character in the MOTD command.
 - B. MOTD banner text may contain only letters and numbers.
 - C. The IOS image on this router does not support the MOTD configuration shown.
 - D. The MOTD delimiting character appeared in the body of the text.
 - E. The banner message exceeds the number of characters allowed.
7. In order to allow the establishment of a Telnet session with a router, which set of commands must be configured?
- A. router(config)# line console 0
router(config-line)# enable password cisco
 - B. router(config)# line console 0
router(config-line)# enable secret cisco
router(config-line)# login
 - C. router(config)# line console 0
router(config-line)# password cisco
router(config-line)# login
 - D. router(config)# line vty 0
router(config-line)# enable password cisco

E. router(config)# line vty 0
 router(config-line)# enable secret cisco
 router(config-line)# login

F. router(config)# line vty 0
 router(config-line)# password cisco
 router(config-line)# login

8. Which two passwords must be supplied in order to connect by Telnet to a properly secured Cisco switch and make changes to the device configuration? (Choose two.)

- A. console password
- B. vty password
- C. aux password
- D. tty password
- E. enable secret password
- F. username password

9. This graphic shows the results of an attempt to open a Telnet connection to router ACCESS1 from router Remote27. Which of the following command sequences will correct this problem?

```
Remote27#
Remote27#telnet access1
Trying ACCESS1 (10.0.0.1)... Open

Password required, but none set

[Connection to access1 closed by foreign host]
Remote27#
```

- A. ACCESS1(config)# line console 0
 ACCESS1(config-line)# password cisco
- B. Remote27(config)# line console 0
 Remote27(config-line)# login
 Remote27(config-line)# password cisco
- C. ACCESS1(config)# line vty 0 4
 ACCESS1(config-line)# login
 ACCESS1(config-line)# password cisco
- D. Remote27(config)# line vty 0 4
 Remote27(config-line)# login
 Remote27(config-line)# password cisco
- E. ACCESS1(config)# enable password cisco
- F. Remote27(config)# enable password cisco

10. Refer to the exhibit. What is the meaning of the output MTU 1500 bytes?

```
Router# show interfaces ethernet 0
Ethernet0 is up, line protocol is up
Hardware is QUICC Ethernet, address is 00c0.ab73.dead (bia 0010.7bcc.7321)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
<output omitted>
Router#
```

- A. The maximum number of bytes that can traverse this interface per second is 1500.

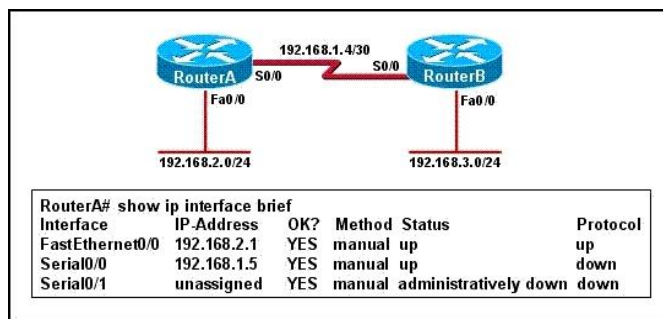
- B. The minimum segment size that can traverse this interface is 1500 bytes.
- C. The maximum segment size that can traverse this interface is 1500 bytes.
- D. The minimum packet size that can traverse this interface is 1500 bytes.
- E. The maximum packet size that can traverse this interface is 1500 bytes.
- F. The maximum frame size that can traverse this interface is 1500 bytes.

11. The show interfaces serial 0/0 command resulted in the output shown in the graphic. What are possible causes for this interface status? (Choose three.)

```
Router#show interfaces serial0/0
Serial0/0 is up, line protocol is down
  Hardware is HD64570
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
```

- A. The interface is shut down.
- B. No keepalive messages are received.
- C. The clockrate is not set.
- D. No loopback address is set.
- E. No cable is attached to the interface.
- F. There is a mismatch in the encapsulation type.

12. Refer to the exhibit. Hosts in network 192.168.2.0 are unable to reach hosts in network 192.168.3.0. Based on the output from RouterA, what are two possible reasons for the failure? (Choose two.)



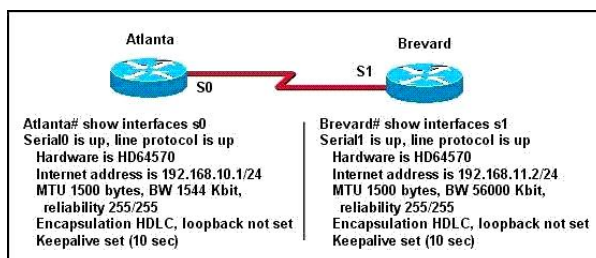
- A. The cable that is connected to S0/0 on RouterA is faulty.
- B. Interface S0/0 on RouterB is administratively down.
- C. Interface S0/0 on RouterA is configured with an incorrect subnet mask.
- D. The IP address that is configured on S0/0 of RouterB is not in the correct subnet.
- E. Interface S0/0 on RouterA is not receiving a clock signal from the CSU/DSU.
- F. The encapsulation that is configured on S0/0 of RouterB does not match the encapsulation that is configured on S0/0 of RouterA.

13. What is the purpose of using the traceroute command?

- A. to map all the devices on a network
- B. to display the current TCP/IP configuration values

- C. to see how a device MAC address is mapped to its IP address
- D. to see the path a packet will take when traveling to a specified destination
- E. to display the MTU values for each router in a specified network path from a source to a destination

14. Two routers named Atlanta and Brevard are connected by their serial interfaces as shown in the exhibit, but there is no data connectivity between them. The Atlanta router is known to have a correct configuration. Given the partial configurations shown in the exhibit, what is the problem on the Brevard router that is causing the lack of connectivity?



- A. A loopback is not set.
- B. The IP address is incorrect.
- C. The subnet mask is incorrect.
- D. The serial line encapsulations are incompatible.
- E. The maximum transmission unit (MTU) size is too large.
- F. The bandwidth setting is incompatible with the connected interface.

15. When upgrading the IOS image, the network administrator receives the exhibited error message. What could be the cause of this error?

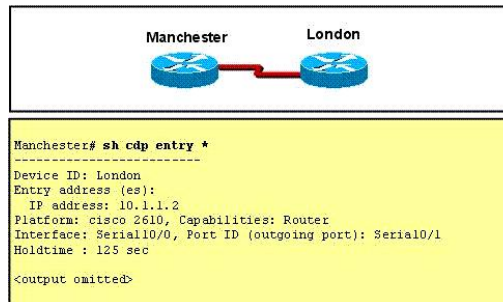
```
Router#copy tftp flash
Address or name of remote host []? 192.168.1.5
Source filename []? c1841-js-1-121-3.bin
Destination filename [c1841-js-1-121-3.bin]?
Accessing tftp://192.168.1.5/c1841-js-1-121-3.bin.....
%Error opening tftp://192.168.1.5/c1841-js-1-121-3.bin (Timed out)
```

- A. The new IOS image is too large for the router flash memory.
- B. The TFTP server is unreachable from the router.
- C. The new IOS image is not correct for this router platform.
- D. The IOS image on the TFTP server is corrupt.
- E. There is not enough disk space on the TFTP server for the IOS image.

16. What are two reasons a network administrator would use CDP? (Choose two.)

- A. to verify the type of cable interconnecting two devices
- B. to determine the status of network services on a remote device
- C. to obtain VLAN information from directly connected switches
- D. to verify Layer 2 connectivity between two devices when Layer 3 fails
- E. to obtain the IP address of a connected device in order to telnet to the device
- F. to determine the status of the routing protocols between directly connected routers

17. Refer to the exhibit. The two exhibited devices are the only Cisco devices on the network. The serial network between the two devices has a mask of 255.255.255.252. Given the output that is shown, what three statements are true of these devices? (Choose three.)



- A. The Manchester serial address is 10.1.1.1.
- B. The Manchester serial address is 10.1.1.2.
- C. The London router is a Cisco 2610.
- D. The Manchester router is a Cisco 2610.
- E. The CDP information was received on port Serial0/0 of the Manchester router.
- F. The CDP information was sent by port Serial0/0 of the London router.

18. Refer to the exhibit. Assuming that the router is configured with the default settings, what type of router interface is this?

```
R1#show interfaces <<output omitted>>
<<output omitted>> is up, line protocol is up
Hardware is Lance, address is 0010.7b80.bfa6 (bia 0010.7b80.bfa6)
MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
<<output omitted>>
```

- A. Ethernet
- B. FastEthernet
- C. Gigabit Ethernet
- D. asynchronous serial
- E. synchronous serial

19. Refer to the exhibit. Which two statements are true of the interfaces on Switch1? (Choose two.)

```
Switch1# show mac address-table
Total MAC addresses: 50
Not-Static Address Table:
Destination Address    AddressType    VLAN    Destination Port
-----
0010.00e0.e289         Dynamic        1        FastEthernet0/1
0010.7b00.1540         Dynamic        2        FastEthernet0/5
0010.7b00.1545         Dynamic        2        FastEthernet0/5
0010.5cf4.0076         Dynamic        1        FastEthernet0/1
0010.5cf4.0077         Dynamic        3        FastEthernet0/1
0010.5cf4.1315         Dynamic        1        FastEthernet0/1
0010.70cb.f301         Dynamic        2        FastEthernet0/1
0010.70cb.3601         Dynamic        5        FastEthernet0/2
0010.1e42.9978         Dynamic        4        FastEthernet0/1
0010.1e9f.3900         Dynamic        3        FastEthernet0/1
0010.70cb.33f1         Dynamic        6        FastEthernet0/3
0010.70cb.103f         Dynamic        6        FastEthernet0/4
<output omitted>

Switch1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID    Local Intrfce    Holdtime    Capability    Platform    Port ID
Switch2      Fas 0/1          157         S             2950-12     Fas 0/1
Switch3      Fas 0/2          143         S             2950-12     Fas 0/5
Switch1#
```

- A. Multiple devices are connected directly to FastEthernet0/1.
- B. A hub is connected directly to FastEthernet0/5.
- C. FastEthernet0/1 is connected to a host with multiple network interface cards.
- D. FastEthernet0/5 has statically assigned MAC addresses.
- E. FastEthernet0/1 is configured as a trunk link.
- F. Interface FastEthernet0/2 has been disabled.



4.7 真题解答***

1. 解：D

题目问：在路由器的 NVRAM 配置中，没有 boot system 命令，在路由器的重启过程中，加载 IOS 的顺序是什么？这里问的是路由器加载 IOS 的过程，可以参照本章的 4.2.2 节，该过程顺序如下：

(1) 路由器在 POST 后，先查看寄存器的值，这个值是一组 4 个十六进制的数字，而其中的最后一个十六进制数影响启动的过程，0x0000 指定路由器进入 ROM 监控模式，0x0001 指定从 ROM 中启动，0x0002~0x000F 的值则参照在 NVRAM 配置文件中 boot system 命令指定的顺序。这里没有提到该值，现实中一般也不使用该值，所以跳过这步。

(2) 在 NVRAM 的配置文件中查看 boot system 命令，这个命令告诉引导程序在哪里寻找 IOS。在这个题中说没有 boot system 命令保存在 NVRAM 中，所以跳过这步。

(3) 如果在 NVRAM 的配置文件中没有找到 boot system 命令，引导程序使用 flash 中所找到的第一个有效的 IOS 镜像。

(4) 如果 flash 中没有有效的 IOS 镜像，引导程序将生成一个 TFTP 本地广播以定位 TFTP 服务器。

(5) 如果没有找到 TFTP 服务器，引导程序将加载 ROM 中的迷你 IOS (RXBOOT 模式)。

(6) 如果 ROM 中有迷你 IOS，那么迷你 IOS 在随后加载并且进入 RXBOOT 模式；否则路由器加载 ROMMON 并且进入 ROM Monitor 模式。

2. 解：C

题目问：在路由器启动过程中，显示错误信息 “boot:cannot open “flash.””，即引导出错，不能从 flash 中正常加载 IOS，接下来路由器将做什么？本题与第 1 题考的都是 IOS 加载的过程，如果路由器从 flash 中加载 IOS 失败，接下来将会尝试从 TFTP 服务器加载 IOS，如果从 TFTP 服务器加载也失败，路由器将进入 ROM Monitor 模式，故正确答案是 C。

3. 解：A

题目问：一台思科路由器重新启动，刚刚完成 POST，准备查找和加载 IOS 文件，路由器接下来执行什么操作？从第 1 题介绍的路由器 IOS 加载过程可知，POST 完成后，路由器将检查配置寄存器的值，故 A 正确。

4. 解：AC

题目问：参照图，因为哪两个原因，路由器从图中显示的位置加载 IOS 镜像文件？从 show version 命令的输出中，可以看到配置寄存器的值是 0x2102，“System image file is tftp://172.16.1.129/Hampton/nitro/c7200-j-mz”这句话表明系统的镜像文件来自 TFTP。从第 1

题的介绍中可以得知,配置寄存器的最后一个十六进制数是 2,表明路由器使用 boot system 中的命令加载 IOS。要么是管理员使用 boot system 命令配置路由器从 TFTP 服务器加载 IOS;要么是路由器在 flash 中找不到一个有效的 IOS 文件,然后使用广播查找 TFTP 服务器,并从 TFTP 服务器加载 IOS。故正确答案是 A 和 C。

5. 解: E

题目问: service password-encryption 命令的影响是什么?可以参照本章的 4.3.5 节,路由器特权密码的配置方式有 enable password 和 enable secret, enable secret 配置的密码被系统加密,使用 show running-config 命令不能看到原始的密码,而 enable password 的密码却是明文显示,可以使用 service password-encryption 命令对路由器上现有的和将来出现的所有密码进行加密,包括 Console 端口、VTY 接口、enable password、用户名对应的密码等。故 E 选项正确。可以使用 no service password-encryption 命令取消密码加密功能,但 no service password-encryption 命令并不能还原 service password-encryption 命令加密的口令,仅会影响之后输入的密码。

6. 解: D

题目问:管理员使用上面的窗口配置了 MOTD 信息,管理员登录路由器时看到的却是下面窗口显示的信息,为什么想要显示的信息(电话号码等)没有显示出来?读者注意到 MOTD 使用的分界符是“#”,可是“#”出现在电话号码的前面,路由器遇到分界符,即认为 MOTD 信息已经配置完成,结果一些想显示的信息被忽略。故 D 正确。解决的办法是,可以换一种在消息正文中不会出现的分界符,比如“\$”、“@”等。

7. 解: F

题目问:为了建立到路由器的 Telnet 会话,哪一系列的命令必须被配置?本题可以参照本章 4.3.5 节, Telnet 是一个应用层的应用,它使用的是 VTY 线路,在默认的情况下,需要访问的线路下设有密码的,在 VTY 线路下设置密码的命令为 password string,而 VTY 线路下的另一个命令 login 则是默认,可写也可不写。如果想在 Telnet 时在 VTY 线路下不设置密码也可以访问这个线路,可以在该 VTY 线路下输入命令 no login,即不要求验证。

8. 解: BE

题目问:为了可以使用 Telnet 连接到一台安全的思科交换机,并对交换机进行配置,哪两个密码必须配置?本题可以参照本章 4.3.5 节,配置 VTY 线路密码以允许远程登录,配置特权密码以允许远程登录,可以进入特权模式,进而对交换机进行配置。后续章节会介绍到交换机的配置,但思科路由器和交换机远程登录的配置命令相同。

9. 解: C

题目问:图中显示了从 Remote27 路由器远程登录 ACCESS1 路由器,使用什么命令可以解决这个问题? Telnet 在默认情况下是要求 VTY 线路设置密码的,因为在 VTY 线路下默认有 login 设置,表示的是开启认证,因此,如果在 VTY 线路下没有设置密码,就不允许使用 VTY 线路进行访问。所以需要在被访问设备(这里是 ACCESS1)的 VTY 线路下设置一个密码,使用命令 password 就可以了,故正确答案是 C。

10. 解: E

题目问:图中的 MTU 1500 字节是什么意思? MTU 是 Maximum Transmission Unit 的简

写，意指最大传输单元，这里显示的是第三层的 MTU。协议数据单元在第三层被叫做包（packet）。在传输层被叫做分段（segment），到网络层会被加入包头，分段比包小。在数据链路层被叫做帧，帧要对包进行封装，帧比包更大。

11. 解：BCF

题目问：图中显示了 `show interfaces serial 0/0` 命令的输出结果，导致这种接口状态的可能原因是什么（选三个）？读者注意到图中显示的是 `Serial0/0 is up, line protocol is down`，出现这种状态的原因有好多种，这里最好使用排除法。A 选项说接口被关闭，如果接口被关闭，显示的是 `Serial0/0 is administratively down, line protocol is down`，故 A 错；D 选项说，没有设置环回接口的地址，物理接口的状态与环回接口有没有设置没有关系，图中的“`loopback not set`”指的是环回检测，指的是不是环回接口，故 D 选项错；E 选项说接口没有连接线缆，“串行”接口没有连接线缆的显示是 `Serial0/0 is down, line protocol is down`。故正确的答案是 BCF。串行接口的状态为一个 up 一个 down，可能出现的情况有：没有收到 `keepalive` 的报文，或者接口的时钟频率没有设置，或者接口封装不匹配，这些都有可能导致接口的协议层 down，这里的串行口是广域网接口，本书广域网部分会介绍到接口时钟和封装类型配置。

12. 解：EF

题目问：192.168.2.0 网络的主机不能到达 192.168.3.0 网络的主机，基于图中 RouterA 的输出，导致失败的原因可能是哪两个？RouterA 的线路故障或 RouterB 的接口没有打开，RouterA Serial0/0 接口的状态都应该是 down down，而图中显示的是 up down，可以排除选项 A 和 B。选项 C 和 D 说两端的 IP 地址或子网掩码不正确，IP 和子网掩码的配置，不影响接口协议的 up 或 down，可以排除选项 C 和 D。正确的答案是 E 和 F。本书广域网部分会进一步介绍时间配置和接口封装协议。

13. 解：D

题目问：使用 `tracert` 命令的目的是什么？参照本章 4.4.1 节的 `tracert` 命令显示，`tracert` 是思科路由器和交换机上的追踪命令，用来显示到达某个特定目标地址所通过的路径，该命令会显示所经过的每一跳路由器地址。用在 Windows 操作系统上的 DOS 命令是 `tracert`。

14. 解：B

题目问：路由器 Atlanta 和 Brevard 通过串行线相连，但路由器间的数据通信失败。路由器 Atlanta 的配置正确，图中给出了部分输出，路由器 Brevard 的什么错误导致两端的通信失败？这是很明显的错误，两台路由器的串行接口的 IP 地址不在相同的网段，从而导致不能通信，路由器 Brevard 接口的 IP 地址配置错误。故正确答案选 B。

15. 解：B

题目问：当更新 IOS 文件时，管理员收到图中提示的错误信息“`error opening tftp……(timed out)`”，是什么导致了错误？从图中的显示可以判断，更新 IOS 失败的原因是路由器无法连接到 TFTP 服务器。既然 TFTP 服务器都无法连接，更不可能知道 IOS 文件的大小及文件是否正确，也无法衡量路由器的 flash 空间是否能满足要求。从 TFTP 服务器往路由器上拷贝文件，与 TFTP 服务器空间大小无关。

16. 解: DE

题目问: 管理员使用 CDP 协议的两个原因是什么? CDP 是一个二层的协议, 因此可以检测二层的连通性, 而且还可以检测到三层的 IP 地址。如果链路出现了故障, 可以通过 CDP 来检测是否是二层出现了故障。同时也可以查看到邻居设备的 IP 地址, 来实现 Telnet 的应用。

17. 解: ACE

题目问: 图中的两台路由器都是思科公司生产的, 两台路由器间通过串行线相连, 子网的掩码是 255.255.255.252, 在 Manchester 路由器上使用 `show cdp entry *` 命令, 显示如图所示, 问哪三个语句的叙述是正确的? CDP 是 Cisco 私有的一个二层的协议, 但是它却可以发现三层的 IP 信息。通过 CDP 可以发现的邻居信息有: 设备的名称、IP 地址、端口、能力、平台、对端的 Holddown time 等。从图中 `show cdp entry *` 命令的显示, 可以看到的的信息有: 设备名称: London; IP 地址: 10.1.1.2; 平台: Cisco 2610; 能力: Router; 端口: S0/1; Holdtime: 123s; Manchester 收到这个 CDP 信息的接口为 S0/0。10.1.1.2 255.255.255.252 属于 10.1.1.0/30 子网, 这个子网中有两个 IP 地址可以使用, 即 10.1.1.1 和 10.1.1.2。综合前面的叙述, 正确的答案是 ACE。

18. 解: B

题目问: 假设路由器使用的是默认配置, 根据图中的输出, 可以判断这个接口是什么类型的接口? 这道题需要根据图中提供的信息来判断接口的类型。可以看到接口的 MAC 地址, 表示这个接口肯定不是串行接口, 所以可以排除选项 D 和 E。带宽 BW 100 000 Kbit, 表示的是 100Mbps 的带宽, 所以这个是 Fast Ethernet 接口。

19. 解: BE

题目问: 根据 Switch1 上的输出, 哪两个选项的叙述是正确的? 本题使用排除法, A 选项说有多个设备被直接连接在 FastEthernet0/1 端口, 交换机的一个端口只能连接一台设备, 这台设备可以是计算机、路由器、集线器或交换机等, 多个设备不可能同时连接在交换机的一个端口上。从 MAC 地址表中和 `show cdp neighbors` 的输出中, 可以得知 FastEthernet0/1 端口连接到 Switch2 的 FastEthernet0/1 端口, Switch2 上连接多台设备, 故 A 错误; B 选项说 Switch1 的 FastEthernet0/5 端口连接一台集线器, 从 MAC 地址表中可以看到, FastEthernet0/5 端口学到两个 MAC 地址, 从邻居表中可以看到, FastEthernet0/5 端口并没有连接一台交换机, 故可以判断 FastEthernet0/5 端口连接的是一台集线器; C 选项说 Switch1 的 FastEthernet0/1 端口连接一台计算机的多块网卡, 这也是不可能的; D 选项说 Switch1 的 FastEthernet0/5 端口配置了静态 MAC 地址, 从 MAC 地址表中看到的都是 “Dynamic” (动态), 并没有看到 “Static” (静态), 故 D 错误; E 选项说 Switch1 的 FastEthernet0/1 端口是一个主干端口, 从 MAC 地址表中可以看到, FastEthernet0/1 端口可以学到多个 VLAN 的 MAC 地址, 故该端口是主干端口; F 选项说 Switch1 的 FastEthernet0/2 端口被禁用, 如果端口被禁用, 该端口对应的 MAC 地址马上被老化, 从 MAC 地址表中可以看到 FastEthernet0/2 端口仍对应的 MAC 地址。

第 5 章

路由选择协议***

本章的主要内容包括：路由原理，直连、静态和默认路由的配置，静态路由与动态路由的区别，动态路由的分类，管理距离的作用和路由选路原则。

5.1 路由基础**

随着计算机网络规模的不断扩大，大型互联网络（如 Internet）的迅猛发展，路由技术在网络技术中已逐渐成为关键部分，路由器也随之成为最重要的网络设备。用户的需求推动着路由技术的发展和路由器的普及，人们已经不满足于仅在本地网络上共享信息，而希望最大限度地利用全球各个地区、各种类型的网络资源。

5.1.1 网络互连*

把一个网络同其他的网络互连起来，从网络中获取更多的信息和向网络中发布自己的消息，是网络互连的最主要的动力。网络的互连有多种方式，其中使用最多的是交换机互连和路由器互连。

1. 交换机互连网络

交换机工作在 OSI 模型中的第二层，即数据链路层。完成数据帧（Frame）的转发，主要目的是在连接的网络间提供透明的通信。交换机的转发依据数据帧中的源地址和目的地址来判断一个帧是否应转发和转发到哪个端口。帧中的地址称为“MAC”地址或“硬件”地址，一般就是网卡的地址。

交换机的作用是把两个或多个网络互连起来，提供透明的通信。网络上的设备看不到交换机的存在，设备之间的通信就如同在一个网上一样方便。由于交换机是在数据帧上进行转发的，因此只能连接相同或相似的网络（相同或相似结构的数据帧），如以太网之间、以太网与令牌环之间的互连，对于不同类型的网络（数据帧结构不同），如以太网与 X.25 之间的互连，交换机就无能为力了。

交换机扩大了网络的规模，提高了网络的性能，给网络应用带来了方便，在以前的网络中，交换机的应用较为广泛。但交换机互连也带来了不少问题：

第一个问题是广播风暴，交换机不能阻挡网络中广播消息，当网络的规模较大时（几个交换机、多个以太网段），有可能引起广播风暴，导致整个网络被广播信息充满，直至完全瘫痪。

第二个问题是网络互连，交换机是数据链路层的设备，无法完成不同 IP 网段间的互连，

也就是不管互连的设备有多少台，这些设备只能在同一个 IP 子网中，如果一个部门和另一个部门处在不同的 IP 子网中，交换机将不能完成网络的互连。

第三个问题是网络安全，交换机无法实现连接不同的 IP 子网，解决的办法就是把两边的网络设备配置在同一个 IP 子网中，当与外部网络互连时，把内部和外部网络合二为一，成为一个网，双方都向对方完全开放自己的网络资源，出于安全考虑，这在很多网络中都是不允许的。

2. 路由器互连网络

路由器互连与网络的协议有关，本书仅讨论 TCP/IP 网络的情况。路由器工作在 OSI 模型中的第三层，即网络层。路由器利用网络层定义的“逻辑”地址（即 IP 地址）来区别不同的网络，实现网络的互连和隔离，保持各个网络的独立性。路由器不转发广播消息，而把广播消息限制在各自的网络内部。发送到其他网络的数据包先被送到路由器，再由路由器转发出去。

IP 路由器只转发 IP 分组，把其余的部分挡在网内（包括广播），从而保持各个网络具有相对的独立性，这样可以组成具有许多网络（子网）互连的大型的网络。由于是在网络层的互连，路由器可方便地连接不同类型的网络，只要网络层运行的是 IP 协议，通过路由器就可互连起来。

网络中的设备用它们的网络地址（TCP/IP 网络中为 IP 地址）互相通信。IP 地址是与硬件地址无关的“逻辑”地址。路由器根据 IP 地址来转发数据，IP 地址的结构有两部分，一部分定义为网络号，另一部分定义为网络内的主机号。目前，在 Internet 网络中采用子网掩码来确定 IP 地址中的网络地址和主机地址。子网掩码与 IP 地址一样，也是 32bit，并且两者是一一对应的，并规定子网掩码中数字为“1”所对应的 IP 地址中的部分为网络号，为“0”所对应的则为主机号。网络号和主机号合起来，才构成一个完整的 IP 地址。同一个网络中的主机 IP 地址，其网络号必须是相同的，这个网络称为 IP 子网。

有相同网络号的主机之间可以直接通信，要与其他 IP 子网的主机进行通信，则必须经过同一网络上的某个路由器或网关（gateway）实现。不同网络号的 IP 地址不能直接通信，即使它们连接在一起，也不能通信。

路由器有多个端口，用于连接多个 IP 子网，每个端口的 IP 地址的网络号要与所连接的 IP 子网的网络号相同。不同的端口对应不同的 IP 子网，路由器多个端口的网络号必须不同。

如表 5-1-1 所示为路由技术和交换技术的比较。

表 5-1-1 路由技术和交换技术的比较

对比项目	路由技术	交换技术
被传输的数据单元	数据包（packet）	帧（frame）
被连接的网络	具有不同物理特性的网络	具有相似物理特性的局域网
网络互连设备	路由器	网桥或交换机

5.1.2 路由原理*

路由选择发生在网络层，主要由路由器来完成，路由器可以将 LAN 连接到 WAN 上，或者将两个使用不同介质访问控制子层的 LAN 连接起来。路由器的工作就是接收信息分组，根据当前网络的状况将其导向最有效的路径。路由器也被称为转存设备，因为它在内存中

存储收到的信息分组，直到它被发送出去。在路由器中的路由表必须实时更新，以准确地反映当前的网络状态，找到一条最合适的分组传送路线。网络拓扑信息可以被网络管理员配置（静态），也可以通过动态方法在网络上收集。

当 IP 子网中的一台主机发送 IP 分组给同一 IP 子网的另一台主机时，它将直接把 IP 分组送到网络上，对方就能收到。而要送给不同 IP 子网上的主机时，它要选择一个能到达目的子网的路由器，把 IP 分组送给该路由器，由路由器负责把 IP 分组送到目的地。一般的主机都配置了“默认网关”（default gateway），“默认网关”是每台主机上的一个配置参数，它是接在同一个网络上的某个路由器端口的 IP 地址，主机把所有未知网络的 IP 分组都发送给“默认网关”，也就是出口路由器。在如图 4-4-1 所示的真实计算机上使用“route print”，显示当前的主机路由，如图 5-1-1 所示，其中上面画线的一行是主机的默认路由，默认路由的出口（192.168.1.1）是和计算机在同一网段的路由设备接口的 IP 地址；下面画线的一行是计算机的本地路由，去往 192.168.1.0 的数据包将直接从网卡发出，不再发往路由器。还可以使用“route add”命令添加路由，“route delete”命令删除路由，有关 route add/delete 命令的使用方法，可以使用“route /?”命令查看在线帮助。

```

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>route print

IPv4 Route Table
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x10003 ...00 0c 29 76 7c 56 ..... AMD PCNET Family PCI Ethernet Adapter
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
-----
0.0.0.0                    0.0.0.0          192.168.1.1      192.168.1.2      30
127.0.0.0                  255.0.0.0        127.0.0.1        127.0.0.1        1
192.168.1.0                255.255.255.0    192.168.1.2      192.168.1.2      30
192.168.1.2                255.255.255.255  127.0.0.1        127.0.0.1        30
192.168.1.255              255.255.255.255  192.168.1.2      192.168.1.2      30
224.0.0.0                  240.0.0.0        192.168.1.2      192.168.1.2      30
255.255.255.255            255.255.255.255  192.168.1.2      192.168.1.2      1
Default Gateway:          192.168.1.1
=====
Persistent Routes:
None

C:\Documents and Settings\Administrator>
    
```

图 5-1-1 主机的路由表

路由器转发 IP 分组时，只根据 IP 分组目的 IP 地址的网络号部分选择合适的端口，把 IP 分组发送出去。同主机一样，路由器也要判定端口所连接的是否是目的子网，如果是，就直接把分组通过端口发送到网络上；否则，也要选择下一个路由器来传送分组。路由器也有它的默认网关，称做默认路由，用来传送不知道往哪里送的 IP 分组。这样，通过路由器把知道如何传送的 IP 分组正确转发出去，不知道的 IP 分组送给“默认网关”路由器，这样一级级地传送，IP 分组最终被送到目的地，送不到目的地的 IP 分组则被网络丢弃。

目前 TCP/IP 网络，全部是通过路由设备互连起来的，Internet 就是成千上万个 IP 子网通过路由设备互连起来的国际性网络。这种网络称为以路由器为基础的网络，形成了以路由器为结点的互联网。在互联网中，路由器不仅负责对 IP 分组的转发，还要负责与其他的路由器进行联络，共同确定互联网的路由选择和维护路由表。

路由包括两个基本动作：寻址和转发。寻址即寻找到达目的地的最佳路径，由路由选择算法来实现。网络中的寻址方式有两种：

- **直接寻址：**源主机与目的主机在相同网络中。在物理网络内部确定主机间的数据传

输路径，不经过路由器。

- **间接寻址**：源主机与目的主机在不同网络中。当主机需要向不在同一网络中的主机发送分组时，主机先要使用数据链路层地址和路由器的一个接口通信。路由器检查接收分组，确定分组的网络，然后参照路由表，决定分组应从哪个接口发送出去，并用外出接口的数据链路层地址进行封装，接着再排队准备被转发，最后在目的网络中用直接寻址方法到达目的主机。

直接寻址发生在第二层，根据物理地址来进行。间接寻址在第三层完成，依据是 IP 地址。路由技术就是指为 IP 数据包在通信子网中寻找传输路径，采用间接寻址方式将数据包逐站传递，直至最终设备。由于涉及不同的路由选择协议和路由选择算法，要相对复杂一些。为了判定最佳路径，首先要选择一种路由协议，不同的路由协议使用不同的度量值。所谓度量值，即判断传输路径好坏的评价标准。度量值包括：跳数（Hop count，即经过路由器的数量）、Bandwidth（带宽）、Delay（延时）、Reliability（可靠性）、Load（负载）、Ticks（滴答数）和 Cost（花费）等。路由选择算法必须启动并维护包含路由信息的路由表，其中路由信息依赖于所用的路由选择算法而不尽相同。路由选择算法将收集到的不同信息填入路由表中，根据路由表可将目的网络与下一站（next-hop）的关系告诉路由器。路由器间互通信息进行路由更新，更新维护路由表使之正确反映网络的拓扑变化，并由路由器根据度量值来决定最佳路径，这就是路由协议（Routing protocol），例如 RIP（Route Information Protocol，路由信息协议）、EIGRP（Enhanced Interior Gateway Routing Protocol，增强型内部网关路由协议）、OSPF（Open Shortest-Path First，开放式最短路径优先协议）和 BGP（Border Gateway Protocol，边界网关协议）等。

转发即沿寻址好的最佳路径传送信息分组。路由器首先在路由表中查找，判明是否知道如何将分组发送到下一个站点（路由器或主机），如果路由器不知道如何发送分组，通常将该分组丢弃；否则就根据路由表的相应表项将分组发送到下一个站点，如果目的网络直接与路由器相连，路由器就把分组直接发送到相应的端口上。

5.1.3 路由协议***

在讲路由协议之前，搞清楚被路由协议和路由协议这两个概念很重要，它们经常出现且容易被混淆，CCNA 考试中要求考生能正确区分路由协议（Routing protocol）和被路由协议（Routed protocol）的区别。

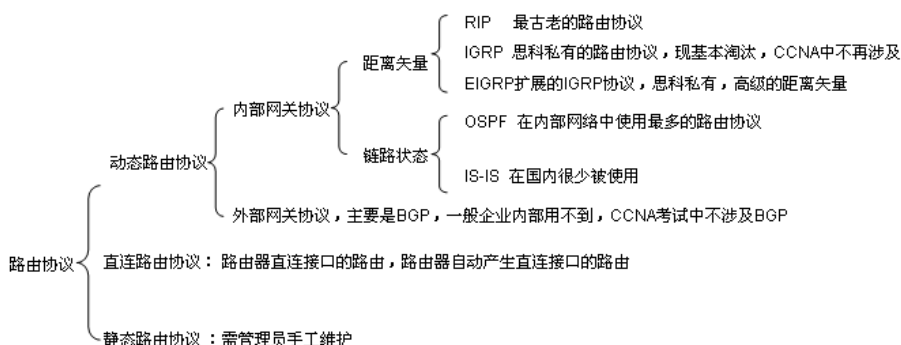
Routing protocol 被翻译成路由协议。路由器使用动态路由协议在互联网上动态发现所有网络，用来构建动态路由表，CCNA 中涉及的路由协议有 RIP、EIGRP、OSPF 等。

Routed protocol 被翻译成被路由协议，有时也称为可路由协议。被路由协议按照路由协议构建的路由表来通过互联网转发用户数据。被路由协议包括 IP、IPX、AppleTalk 等。一个协议要成为可路由的，必须要给每一个设备提供这样的能力，支持网络号和主机号。比如 IPX，只要求分配网络号，因为它们使用主机的 MAC 地址作为主机号；再比如 IP，包括网络号和主机号。而 NetBIOS 仅包括计算机名，是一个不可以被路由的协议。路由器的路由选择是基于目标主机的网络地址，而不是基于目标主机的 IP 地址。

它们是相互配合又相互独立的概念，被路由协议使用路由协议维护的路由表，同时，路由协议要利用被路由协议提供的功能来发布路由协议数据分组。可以把被路由协议想象成卡车，用来运输最终的货物。把路由协议想象成人的大脑，根据货物要到达的目的来

为卡车选择正确的传输路线。

路由协议有直连、静态和动态之分，如图 5-1-2 所示。动态路由协议根据所处的 AS（Autonomic Systems，自治系统）不同，又分为 IGP（Interior Gateway Protocol，内部网关协议）和 EGP（Exterior Gateway Protocol，外部网关协议），这里的自治系统是指一个具有统一管理机构、统一路由策略的网络。IGP 协议是指在同一个 AS 内运行的路由协议，IGP 协议又分为距离矢量路由协议和链路状态路由协议。EGP 协议是指运行在不同 AS 之间的路由协议，目前使用最多的是 BGP 协议，BGP 协议也属于动态路由协议，BGP 协议对配置人员的要求比较高，多数人不会在实际工作环境中遇到，BGP 是 CCNP 中的内容，CCNA 不要求掌握，本书不对 BGP 做过多叙述。



！ 注：EIGRP 是一个高级的距离矢量协议，同时具有距离矢量和链路状态路由协议的特征，有时也被称为混合协议。

5.2 直连路由**

根据路由器学习路由信息、生成并维护路由表的方式，路由分为：直连路由（Connect routing）、静态路由（Static routing）和动态路由（Dynamic routing）。直连路由是由数据链路层协议发现的，是指去往路由器的接口地址所在网段的路径，该路径信息不需要网络管理员维护，也不需要路由器通过某种算法进行计算获得，只要该接口处于激活状态（Active），路由器就会把直连接口所在网段的路由信息填写到路由表中去。

使用 CCNA 机架中的路由器 R1、R2、R3，它们之间的连接和 IP 地址分配如图 5-2-1 所示。本章的实验均在如图 5-2-1 所示的拓扑中完成。

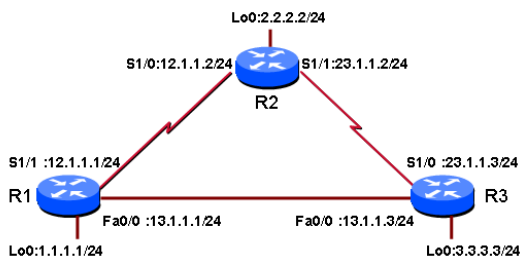


图 5-2-1 网络拓扑图

运行 CCNA 机架中的路由器 R1、R2 和 R3。R1 的具体配置如下：

```
Router>en
Router#conf t
Router(config)#no cdp run
关闭 CDP 协议，不然模拟器中会一直出现双工不匹配的提示信息。以后的实验中只要涉及以太网接口，就关闭 CDP 协议。
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int fa 0/0
R1(config-if)#ip add 13.1.1.1 255.255.255.0
R1(config-if)#int lo0
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config-if)#int s1/2
R1(config-if)#ip add 8.8.8.8 255.255.255.0
R1(config-if)#no shut
```

R2 的具体配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int lo0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
```

R3 的具体配置如下：

```
Router>en
Router#conf t
Router(config)#no cdp run
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int fa 0/0
R3(config-if)#ip add 13.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo0
R3(config-if)#int loopback 0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
```

在路由器 R1 上执行 show ip route 命令，显示 R1 的路由表如下：

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, Loopback0
    12.0.0.0/24 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, Serial1/1
```

从上面的输出可以看出，R1 的路由表中有两个条目：1.1.1.0/24（Loopback 0 接口的直

连路由)和 12.1.1.0/24 (S1/1 接口的直连路由),前面的字母“C”表示的是直连路由,至于为何显示成:

```
1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, Loopback0
```

这样的格式,本书将在“6.5.1 路由结构”一节详细介绍。可却没有发现 Fa0/0 接口的路由(13.1.1.0/24)和 S1/2 接口的路由(8.8.8.0/24),原因是因为路由器会自动产生激活端口的路由,Fa0/0 接口虽然配置了 IP 地址,却没有使用 no shut 命令激活端口,路由表中不会出现该直连接口的路由。有的读者不免会问,Loopback 0 接口也没有使用 no shut 命令,路由表中为何出现了该直连接口的路由,这是因为 Loopback 是虚拟接口,默认是打开的,不需要 no shut 命令。读者还会问为 S1/2 接口配置了 IP 地址,也使用 no shut 命令打开了端口,为何路由表中仍然没有路由,这是因为 S1/2 接口虽然配置了 IP 地址,也打开了端口,但该接口并没有连线,即使该接口连线,如果线缆另一端的设备没有加电或端口没有打开,该接口的 IP 地址仍然是无效的。

在路由器 R2 上执行 show ip route 命令, R2 的路由表显示如下:

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    2.0.0.0/24 is subnetted, 1 subnets
C      2.2.2.0 is directly connected, Loopback0
    23.0.0.0/24 is subnetted, 1 subnets
C      23.1.1.0 is directly connected, Serial1/1
    12.0.0.0/24 is subnetted, 1 subnets
C      12.1.1.0 is directly connected, Serial1/0
```

在路由器 R3 上执行 show ip route 命令, R3 的路由表显示如下:

```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    3.0.0.0/24 is subnetted, 1 subnets
C      3.3.3.0 is directly connected, Loopback0
    23.0.0.0/24 is subnetted, 1 subnets
C      23.1.1.0 is directly connected, Serial1/0
    13.0.0.0/24 is subnetted, 1 subnets
C      13.1.1.0 is directly connected, FastEthernet0/0
```

看到路由器 R3 的路由表,读者可能会问, R1 的 Fa0/0 接口的 IP 地址无效, R3 的 Fa0/0 接口的 IP 地址怎么有效了呢?原因是 R1 和 R3 的 Fa0/0 接口并没有直接连接,中间还有一台交换机。

在路由器 R1 上使用下面的命令激活 Fa0/0 接口:

```
R1(config)#int fa 0/0
R1(config-if)#no shut
```

接下来测试网络的连通性，在路由器 R1 上 “ping 12.1.1.2”，结果显示如下：

```
R1#ping 12.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/24/36 ms
```

在路由器 R1 上 “ping 2.2.2.2”，结果显示如下：

```
R1#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

为何路由器 R1 去往 12.1.1.2 可以到达，去往 2.2.2.2 却失败呢？原因是路由器中数据的流动情况是：当从局域网中接收到一个包时，在进入 RAM 之前，首先检查它的第二层头信息，如果是发往本路由器的，第二层头信息被剥掉，放入 RAM 中。在 RAM 里，路由器检测包第三层的头信息，CPU 同时搜索路由表并匹配第三层地址，以决定包应向哪里输出，以及以怎样的方式进行封装。路由器对本路由器发起的数据包也要查询路由表，决定转发接口。

当在 R1 上 ping 12.1.1.2 时，R1 查询自己的路由表，去 12.1.1.0/24 的包应该从 Serial1/1 接口发出去，R1 和 R2 之间是串行的点对点线路，数据链路层封装 PPP 或 HDLC。R2 收到 R1 发过来的数据包，R2 检查数据包中的目的 IP 地址，发现与本路由器接口的 IP 地址相同，是发往本路由器的。R2 也获知该 ping 包（Echo request）来自 12.1.1.1，R2 查询自己的路由表，把 ping 包的应答包（Echo reply）从 Serial1/0 接口发回去，R1 收到了 R2 的应答包，结果是 R1 成功地 ping 通了 R2。

当在 R1 上 ping 2.2.2.2 时，R1 查询自己的路由表，发现路由表中没有去往 2.2.2.2 的路由，R1 丢弃该数据包，结果是 R1 上 ping 2.2.2.2 失败。

同理，路由器 R1、R2 和 R3 相互之间都可以 ping 通直连接口的 IP 地址，ping 不通非直连的 IP 地址。



5.3 静态路由***

本节介绍静态路由的配置，以及静态路由的优缺点。

5.3.1 配置静态路由***

在 5.2 节中，R1 无法 ping 通 2.2.2.2，有什么办法可以让 R1 能 ping 通该 IP 地址呢？解决的办法之一就是配置静态路由，静态路由就是网段之间的路由需要管理员手工加入。在图 5-2-1 中，如果路由器 R1 知道把去往 2.2.2.2 的数据包发给 R2，R2 查询 ping 包的源 IP 地址，发现是来自 12.1.1.1 的数据包，R2 查询本地的路由表，发现 12.1.1.0/24 是直连路由，R2 把 ping 的应答包从 S1/0 接口发出，R1 收到应答包，ping 成功。关键是管理员如何通知路由器 R1 去往 2.2.2.2 的数据包要发往 R2 呢？这就需要添加静态路由，添加静态路由的命令格式如下：

Ip route	目标网络	掩码	下一跳路由器直连接口的 IP 地址或本路由器的外出接口
administrative_distance	permanent		

“目标网络”是要去往的目标网络地址；“掩码”是目标网络对应的子网掩码；至于使用下一跳路由器直连接口的 IP 地址还是使用本路由器的外出接口，下面有具体的解释；administrative_distance 是管理距离，本章最后一节介绍管理距离。指定了管理距离的静态路由叫做“浮动静态路由”，浮动静态路由在链路备份的场合被广泛使用，本书将在下一章中介绍浮动静态路由的使用；permanent（永久）是一个关键字参数，如果路由器的接口被关闭或和下一跳路由器失去连接，将导致添加的静态路由也从路由表中消失，使用 permanent 参数，不管发生了什么意外情况，该静态路由不会从路由表中消失。

路由器 R1 使用如下的命令，添加去往 2.2.2.0/24 的静态路由。

```
R1(config)#ip route 2.2.2.0 255.255.255.0 12.1.1.2
```

或者

```
R1(config)#ip route 2.2.2.0 255.255.255.0 s1/1
```

对于命令中的 ip route 2.2.2.0 255.255.255.0 12.1.1.2，其中，2.2.2.0 是要到达的目标网络，在静态路由中需要添加所有的非直连网络；255.255.255.0 是目标网络对应的子网掩码；12.1.1.2 是与本路由器直接相连的下一跳路由器的接口地址，这里特别要注意的是，即使要到达的网络与本路由器相隔数台路由器，这里填入的还是下一跳地址，而不是目标网络的前一跳，也就是说，在静态路由中，只需要指出下一跳的地址，至于以后如何指向，那是下一跳路由器考虑的事情。第二条命令中填入的不是 IP 地址，而是路由器 R1 的外出接口。

这两条命令的结果是相同的，都是在 R1 上添加一条去往 2.2.2.0/24 网段的路由。至于填的是下一跳的地址，还是本路由器的外出接口，还是有差别的。

- **区别一：**上面一条命令引用的是下一跳路由器和本路由器相连接口的 IP 地址，该路由的管理距离是 1；下面一条命令引用的是本路由器的外出接口，该路由的管理距离是 0。
- **区别二：**本路由器出口命令仅能用在点对点的链路上，比如本例中的串行线路，串行线路在数据链路层封装的是一种协议，如 HDLC(High Level Data Link Control protocol, 高级数据链路控制协议)或 PPP(Point-to-Point Protocol, 点对点协议)，这两个协议使用在点对点的链路上，一台设备发送数据，另一台设备就能收到；如果串行线路封装的是帧中继(Frame-relay)协议，因为帧中继链路默认是 NBMA(Non-Broadcast Multiple Access, 非广播多路访问)，也是多路访问链路，那时也需要指向下一跳路由器的接口 IP 地址，而不能是外出接口。如果是以太网这种多路访问的链路，指外出接口，路由器将不知道把包发往哪一台路由器，路由器不知道要发往哪一个 IP 地址，自然也就无法完成 ARP 的解析过程，在不知道下一跳设备 MAC 地址的情况下，无法完成 ping 包的数据封装。同理，在多路访问的帧中继链路上，因不知道具体使用哪一条 PVC(Permanent Virtual Circuit, 永久虚电路)，也不能指外出接口。

接下来证明使用本路由器外出口还是使用下一跳路由器接口 IP 地址的区别，顺带讲解第 2 章介绍的 Proxy ARP(代理 ARP)的使用，本章视频部分也有相应的讲解。

使用下面的命令在路由器 R1 上添加静态路由：

```
R1(config)#ip route 2.2.2.0 255.255.255.0 12.1.1.2    或 s1/1
R1(config)#ip route 23.1.1.0 255.255.255.0 13.1.1.3
R1(config)#ip route 3.3.3.0 255.255.255.0 13.1.1.3
```

去往 23.1.1.0/24 的数据包从 R2 和 R3 均可到达，这里选择从 R3 走的原因是因为，R1

和 R3 之间的链路是 100Mb/s, R1 和 R2 之间的链路是 1.544Mb/s。因为以太网是多路访问的网络, 这里只能填下一跳的 IP 地址, 而不能是路由器 R1 的外出接口。值得注意的是, 有的读者配置错误, 这里填成了路由器 R1 的外出接口, 结果却发现 R1 可以 ping 通 23.1.1.3。这里要知道 R1 虽然能 ping 通 R3 的 23.1.1.3, 并不只是配置的静态路由起作用, 还有思科路由器以太网接口的代理 ARP (Proxy ARP) 在起作用, 二者共同起作用, 结果 R1 可以 ping 通。如果在 R1 上不指明外出接口, 路由器 R1 不知道从哪个接口向外广播, ping 失败; 如果 R3 的 Fa0/0 接口开启 Proxy ARP, 路由器 R3 收到 R1 发过来的广播包, 请求的源 IP 地址是 13.1.1.1, 和路由器 R3 接收到广播的 Fa0/0 接口的 IP 地址 13.1.1.3 处在同一网段, 且 R3 上有去往 23.1.1.0/24 的路由, 这就满足了代理 ARP 执行的两个条件:

- 条件一: ARP 请求的源 IP 地址和路由器接口的 IP 地址处在同一个子网中。
- 条件二: 路由器有 ARP 请求的 IP 地址的路由。

路由器 R3 用自己 Fa0/0 接口的 MAC 地址作为应答。有关这一点可以通过下面的命令取消前面的配置:

```
R1(config)#no ip route 23.1.1.0 255.255.255.0 13.1.1.3
R1(config)#no ip route 3.3.3.0 255.255.255.0 13.1.1.3
```

换成:

```
R1(config)#ip route 23.1.1.0 255.255.255.0 Fa0/0
R1(config)#ip route 3.3.3.0 255.255.255.0 Fa0/0
```

然后在路由器 R1 上分别 ping 3.3.3.3 和 ping 23.1.1.3, 结果可以 ping 通, 使用 show arp 命令进行验证, 显示结果如下:

```
R1#show arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 3.3.3.3          1         cc09.0b04.0000 ARPA    FastEthernet0/0
Internet 13.1.1.1         -         cc07.0b04.0000 ARPA    FastEthernet0/0
Internet 13.1.1.3        16        cc09.0b04.0000 ARPA    FastEthernet0/0
Internet 23.1.1.3         0         cc09.0b04.0000 ARPA    FastEthernet0/0
```

从上面的输出中可以看到 3.3.3.3 和 23.1.1.3 都出现在 R1 的 ARP 缓存中, 对应的 MAC 地址都是路由器 R3 Fa0/0 接口的 MAC 地址。使用下面的命令清除路由器 R1 的 ARP 缓存:

```
R1#clear arp
```

再关闭路由器 R3 的代理 ARP, 命令如下:

```
R3(config)#int fa 0/0
R3(config-if)#no ip proxy-arp
```

再次在路由器 R1 上 ping 3.3.3.3 和 ping 23.1.1.3, 结果 ping 不通了。通过上面的操作, 验证了在多路访问的情况下, 配置静态路由只能用下一跳, 而不能使用本路由器的外出接口, 有关这一点, 读者一定要记住, 因为笔者发现很多讲师和工程师都容易忽视这一点。

使用下面的命令在路由器 R2 上添加静态路由:

```
R2(config)#ip route 1.1.1.0 255.255.255.0 12.1.1.1 或 S1/0
R2(config)#ip route 3.3.3.0 255.255.255.0 23.1.1.3 或 S1/1
R2(config)#ip route 13.1.1.0 255.255.255.0 12.1.1.1
或 S1/0, 或 23.1.1.3, 或 S1/1 均可, 也就是去往 13.1.1.0/24 网段, 从 R2 和 R3 走没有区别。
```

使用下面的命令在路由器 R3 上添加静态路由:

```
R3(config)#ip route 2.2.2.0 255.255.255.0 23.1.1.2 或 S1/0
R3(config)#ip route 1.1.1.0 255.255.255.0 13.1.1.1
考虑 R3 和 R1 之间是 100Mb/s, R3 和 R2 之间是 1.544Mb/s, 所以优先考虑使用 R1, 从 100Mb/s 链路走。
R3(config)#ip route 12.1.1.0 255.255.255.0 13.1.1.1 同上
```

本例的实验配置并不是唯一的，比如 R1 去往 2.2.2.2 的路由完全可以不从 R2 走，而从 R3 绕过去，这样配置起来就更复杂了，其实读者可以考虑一种顺时针的配置方法，也就是 R1 去任何地方的数据包都发给 R2，R2 去任何地方的数据包都发给 R3，R3 去任何地方的数据包都发给 R1，这样配置起来相对容易点，但路由走向并不是最优路径，本书中只给出了一种配置方法。

下面总结一下配置静态路由的一般步骤。

步骤 1：为路由器每个接口配置 IP 地址。

步骤 2：确定本路由器有哪些直连网段。

步骤 3：确定网络中有哪些属于本路由器的非直连网段。

步骤 4：在路由表中添加所有非本路由器直连网段的相关路由信息。

另外，静态路由也支持路由汇总，路由汇总的作用是减小路由表的大小，在某些场合还能提高网络的稳定性。在图 5-3-1 中，路由器 R1 需要访问路由器 R2 上的 192.168.1.0、192.168.2.0、192.168.3.0 的网络，需要在路由器 R1 上添加 3 条静态路由。

```
R1(config)#ip route 192.168.1.0 255.255.255.0 12.1.1.2
R1(config)#ip route 192.168.2.0 255.255.255.0 12.1.1.2
R1(config)#ip route 192.168.3.0 255.255.255.0 12.1.1.2
```

也可以使用下面的汇总命令来完成 R1 的配置：

```
R1(config)#ip route 192.168.0.0 255.255.0.0 12.1.1.2
```

这样 R1 上去往 192.168.0.0/16 的数据包都将被发往路由器 R2，这里的汇总属于不精确汇总，还可以汇总成 192.168.0.0/22，不过仍然是不精确汇总，因为 192.168.0.0/22 包含了 4 条路由 192.168.0.0/24、192.168.1.0/24、192.168.2.0/24、192.168.3.0/24，192.168.0.0/24 也被包括进来了。有关路由汇总的方法请参考第 2 章的 IP 计算部分。

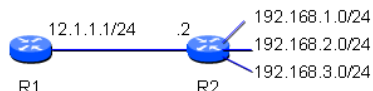


图 5-3-1 静态路由汇总

5.3.2 静态路由的优缺点**

经过前面的学习，读者已经掌握了静态路由的配置。同所有路由协议一样，静态路由协议也有自己的优缺点。了解每种路由协议的优缺点，有利于根据网络规模的状况，正确地选择适合的路由协议。静态路由具有以下优点：

- **对 CPU、内存等硬件的需求不高。**静态路由不像动态路由协议，需要缓存相互间交换的路由信息，并执行一些算法，这意味着静态路由对 CPU 和内存的要求不高。
- **不占用带宽。**静态路由不像动态路由协议，需要相互间交换网络信息或路由表，这意味着静态路由可以节省带宽。
- **增加网络安全。**静态路由是网络管理员手工添加的，即使不同的网络之间存在物理路径，只要管理员没有添加它们之前的静态路由，网络也是不可达的。不像动态路由协议，不容易实现网络间的控制。

静态路由具有以下缺点：

- **配置工作量大且容易出错。**由于所有的路由都需要管理员手工加入，对大型网络来说，这几乎是不可能的，而且容易出错。当某个新的网络出现时，管理员必须在所有路由器上添加这条静态路由。
- **适应拓扑变化的能力较差。**回想图 5-2-1 中路由器 R1、R2 和 R3 的静态路由配置，如果断开路由器 R1 和 R3 之间的链路，将导致路由器 R1 无法到达 3.3.3.3，事实上

R1 是有物理路径可以到达 3.3.3.3 的，那就是从 R2 绕行，可是静态路由不能适应网络拓扑的变化，动态地调整路由走向。



5.4 默认路由**

默认路由 (Default routing) 在有些文档中也称做缺省路由，使用默认路由可以转发那些不在路由表中列出的远端目的网络的数据包到下一跳路由器。在存根网络（只有一条连接到其邻居网络的网络，进、出这个网络都只有一条路可以走）上可以使用默认路由，因为这些网络与外界之间只有一个连接。如图 5-4-1 所示是某公司的网络拓扑，该公司通过路由器接入 ISP，通过 ISP 路由器 218.1.1.1 访问整个 Internet。如果使用的是基于类的静态路由，则需要在公司出口路由器上添加所有的 A 类、B 类、C 类 IP 地址，一般低端的路由器根本无法承受如此多的路由条目。针对图 5-4-1 中的网络拓扑，公司路由器最好的配置方法是使用默认路由，默认路由的配置方法与静态路由类似，只是网络地址和子网掩码改成了“0.0.0.0 0.0.0.0”，即 8 个 0。公司出口路由器默认路由的配置如下：

```
Router(config)#ip route 0.0.0.0 0.0.0.0 218.1.1.1
```

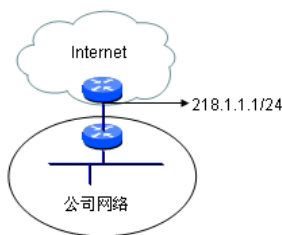


图 5-4-1 存根网络

其实不止是在存根网络上使用静态路由，据统计 Internet 上 99.9% 的路由器都使用了默认路由。4.4.1 节的配置中就使用到了默认路由，本章 5.2 节针对图 5-2-1 中的配置也可以使用默认路由来实现。在路由器 R1、R2 和 R3 上使用“show running-config”命令，查看路由器的配置，使用前加“no”的命令取消所有的“ip route”命令。这里介绍一种取消配置的方法，可以把相关的配置拷贝出来，然后在记事本中用“no ip route”替换“ip route”，再复制、粘贴回路由器。取消静态路由配置命令后，使用如下命令配置路由器 R1、R2 和 R3：

```
R1(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.2    R1 上所有未知的数据包都发给路由器 R2。
R2(config)#ip route 0.0.0.0 0.0.0.0 23.1.1.3    R2 上所有未知的数据包都发给路由器 R3。
R3(config)#ip route 0.0.0.0 0.0.0.0 13.1.1.1    R3 上所有未知的数据包都发给路由器 R1。
```

在路由器 R1 上 ping 图 5-2-1 中的所有 IP 地址，结果均可以 ping 通。在路由器 R1 上使用 traceroute 命令验证数据包的流向，结果显示如下：

```
R1#traceroute 3.3.3.3

Type escape sequence to abort.
Tracing the route to 3.3.3.3

 0  12.1.1.2  20 msec 104 msec 64 msec
 1  23.1.1.3 180 msec 164 msec *
```

从上面的输出中可以看出，路由器 R1 把去往 3.3.3.3 的未知数据包转发给路由器 R2，路由器 R2 再把未知的数据包转发给 R3。R3 返回 R1 的数据包是如何流向的呢？R3 也是走默认路由，把 R1 来的数据包直接发回 R1，也就是说，在 R1 ping R3 的过程中，去的 Echo request 包从 R2 绕过去，回来的 Echo reply 数据包直接返回 R1。traceroute 命令看不到这个结果，可以使用扩展的 ping 命令查看结果，CCNA 考试中不涉及这一知识点，读者了解一下就可以了。

```
R1#ping
Protocol [ip]:
```

```

Target IP address: 3.3.3.3
Repeat count [5]: 1
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: R
这里的 R 表示的是 Record, 记录每一台设备的发起 IP 地址。
Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet has IP options: Total option bytes= 39, padded length=40
Record route: <*>
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)

Reply to request 0 (152 ms). Received packet has options
Total option bytes= 40, padded length=40
Record route:
(12.1.1.1)
(23.1.1.2)
(3.3.3.3)
(13.1.1.3)
(12.1.1.1) <*>
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
(0.0.0.0)
End of list

Success rate is 100 percent (1/1), round-trip min/avg/max = 152/152/152 ms

```

接下来讨论一下路由环路问题。在上面的配置中，如果在 R1 上随便 ping 一个不存在的 IP 地址，比如 9.9.9.9，会出现什么问题呢？显示如下：

```

R1#ping 9.9.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.9.9.9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

```

结果是超时。下面使用 traceroute 命令查看一下 ping 包的发送情况，路由器 R1 的执行如下：

```

R1#traceroute 9.9.9.9

Type escape sequence to abort.
Tracing the route to 9.9.9.9

 1 12.1.1.2 40 msec 16 msec 12 msec
 2 23.1.1.3 244 msec 140 msec 156 msec
 3 13.1.1.1 272 msec 144 msec 48 msec

```

R1 把未知的数据包发给路由器 R2。
R2 把未知的数据包发给路由器 R3。
R3 把未知的数据包发给路由器 R1。

```

4 12.1.1.2 160 msec 168 msec 116 msec
R1 把未知的数据包发给路由器 R2，至此路由环路产生。数据包在路由器 R1→R2→R3→R1→R2...之间
循环转发。
5 23.1.1.3 248 msec 132 msec 72 msec
省略 6~27 跳。
28 12.1.1.2 460 msec 192 msec 148 msec
29 23.1.1.3 140 msec 144 msec 208 msec
30 13.1.1.1 148 msec 240 msec 168 msec
R1#

```

从 traceroute 命令的输出中，可以看出路由环路已经形成，并不是上面的数据包经过 30 跳就终止，而是因为 traceroute 只追踪到 TTL=30。换成 ping 产生的 Echo Request 数据包不会在网络中无休止地发送下去呢？回答是不会，因为网络层的数据包中有一个字段 TTL，TTL 最大值是 255，每经过一台路由器，TTL 至少减 1，当 TTL 减小到 0 时，数据包被丢弃。也就是说，网络层的数据包最多经过 255 台路由器将会被丢弃，不会在网络中无休止地被转发。



5.5 动态路由协议***

前面介绍了直连、静态和默认路由的配置。通过静态路由虽然可以实现网络的互连，但如果网络规模很大，假设有 100 台路由器，101 个网络，每台路由器上有两个直连网络，那么需配置静态路由的条目是 $100 \times (101-2) = 9900$ 条，通过手工几乎无法实现。另外，当网络出现变化时，静态路由也不能很好地反映拓扑变化，这都需要使用动态路由协议。

5.5.1 静态路由与动态路由的比较**

前面介绍过，静态路由是由管理员在路由器中手工添加的路由条目。除非网络管理员干预，否则静态路由不会发生变化。由于静态路由不能对网络的改变做出反应，一般被用于网络规模不大、拓扑结构固定的网络中。静态路由的优点是简单、高效、可靠。

动态路由是网络中的路由器之间相互通信，传递路由信息，利用收到的路由信息更新路由器表的过程。它能实时地适应网络结构的变化，如果路由更新信息表明发生了网络变化，路由选择软件就会重新计算路由，并发出新的路由更新信息。这些信息通过各个网络，引起各路由器执行路由算法，并更新各自的路由表以动态地反映网络拓扑变化。动态路由适用于网络规模大、网络拓扑复杂的网络。当然，各种动态路由协议会不同程度地占用网络带宽和 CPU 资源。

静态路由与动态路由的比较，如表 5-5-1 所示。

表 5-5-1 静态路由与动态路由的比较

	动态路由	静态路由
配置的复杂性	随着网络规模的增加不明显	随着网络规模的增加急剧增强
对管理员的技术要求	相对较高	相对较低
拓扑改变	自动适应拓扑的改变	需要管理员的手工干预
适用环境	简单和复杂的网络	简单的网络
安全性	较低	较高
资源使用	使用 CPU、内存、链路带宽	不使用额外的资源

5.5.2 管理距离***

管理距离（Administrative Distance，简称 AD），有的文档中也翻译成管辖距离，是用来衡量路由可信度的一个参数。管理距离越小，路由越可靠，这意味着具有较小管理距离的路由将优于较大管理距离的路由，管理距离的取值范围为 0~255 的整数值，0 是最可信的，255 是最不可信的。如果一台路由器收到同一个网络的两个路由更新信息，路由器将把管理距离小的路由放入路由表中。表 5-5-2 列出了思科所支持协议的默认管理距离值。

表 5-5-2 思科所支持协议的默认管理距离值

路 由 源	默认管理距离值
直连接口*	0
静态路由（使用外出口）*	0
静态路由（使用下一跳 IP）*	1
EIGRP 汇总路由*	5
外部 BGP	20
内部 EIGRP*	90
IGRP*	100
OSPF*	110
IS-IS（中间系统到中间系统）	115
RIP*	120
EGP（外部网关协议）	140
外部 EIGRP	170
内部 BGP	200
未知*	255

注：CCNA 中只要掌握标*的路由源的管理距离即可。

5.5.3 路由选路原则***

当一个目标地址被多个目标网络覆盖、一个目标网络的多种路由协议的多条路径共存时，或者当一个目标网络同一种路由协议的多条路径共存时，路由器应该如何进行路由的选择？这一部分内容经常被 CCNA 考到，出现的形式大多是列出路由表的多个条目，然后问去往某一个 IP 地址的数据包将发往哪里？

牢记本节的路由选路原则，这样的问题将迎刃而解。路由器依照下列的选路原则进行路由选择。

（1）子网掩码最长匹配

也就是如果一个目标地址被多个目标网络覆盖，它将优先选择最长的子网掩码的路由，匹配得更精确。比如到达 10.0.0.1 的网络有两个：10.0.0.0/24 的下一跳是 12.1.1.2，10.0.0.0/16 的下一跳是 13.1.1.3，则路由器更相信子网掩码长的 10.0.0.0/24 的路由，因为掩码长度 24 大于 16，路由器把数据包发往 12.1.1.2。如果路由器上有发往 10.0.1.1 的数据包，将选择 10.0.0.0/16 路由，因为目标地址 10.0.1.1 不包括在路由条目 10.0.0.0/24 内。

（2）管理距离最小优先

在子网掩码长度相同的情况下，路由器优先选择管理距离小的路由。比如，到达

10.1.1.0/24 的路由有两条，一条是通过 RIP 学习来的，另外一条是通过 OSPF 学习来的，则路由器相信 OSPF 学习来的路由，因为它有更小的管理距离 110，RIP 的管理距离是 120。

RIP 和 OSPF 学来的有关 10.0.0.0/24 的路由会不会同时出现在路由表中呢？回答是不会，因为路由器中只保存最优的路由，只有 OSPF 学到的路由会出现在路由表中，如果 OSPF 学到的路由消失，RIP 学到的路由将出现在路由表中。这一条和第一条是没有冲突的，路由条目 10.0.0.0/16 和 10.0.0.0/24 的掩码长度不同，它们是不同的路由条目，不同的路由条目当然可以同时存在路由表中。

（3）度量值最小优先

如果路由的子网掩码长度相同，管理距离也相等，接下来比较的就是度量值。比如路由器通过 RIP 路由协议学到了 10.0.0.0/24 的两个条目，一个条目的跳数（hop）是 2，另一个条目的跳数是 3，RIP 将使用哪一个条目呢？RIP 比较的是跳数，跳数越少越优先。跳数是 2 的条目将被添加到路由表中，跳数是 3 的条目不会出现在路由表中，如果跳数是 2 的路由条目消失，跳数是 3 的路由条目才会出现在路由表中。

5.5.4 距离矢量和链路状态路由协议***

IGP 路由协议可以被分为两类：距离矢量（Distance vector）和链路状态（Link state）。

距离矢量和链路状态采用了不同的路由算法，路由算法在路由协议中起着至关重要的作用，采用何种算法往往决定了最终的寻径结果，因此选择路由算法一定要仔细。通常需要综合考虑以下几个设计目标：

- **最优化**：指路由算法选择最佳路径的能力。
- **简洁性**：算法设计简洁，利用最少的开销，提供最有效的功能。
- **坚固性**：路由算法处于非正常或不可预料的环境时，如硬件故障、负载过高或操作失误时，都能正确运行。由于路由器分布在网络连接点上，所以在它们出故障时会产生严重后果。最好的路由器算法通常能经受住时间的考验，并在各种网络环境下被证实是可靠的。
- **快速收敛（Convergence）**：路由收敛是指路由域中所有路由器对当前的网络结构和路由转发达成一致的状态。收敛时间是指从网络的拓扑结构发生变化到网络上所有的相关路由器都得知这一变化，并且相应地做出改变所需要的时间。当某个网络事件引起路由可用或不可用时，路由器就发出更新信息。路由更新信息遍及整个网络，引发重新计算最佳路径，最终达到所有路由器一致公认的最佳路径。收敛慢的路由算法会造成路径环路或网络中断。
- **灵活性**：路由算法可以快速、准确地适应各种网络环境。例如，某个网段发生故障，路由算法要能很快发现故障，并为使用该网段的所有路由选择另一条最佳路径。

1. 距离矢量路由协议

距离矢量路由选择算法定期地将路由表的拷贝从一个路由器发往另一个路由器。这些在路由器间的定期更新交流了网络的路由信息和变化，基于距离矢量的路由选择算法也称为贝尔曼-福特（Bellman-Ford）算法。RIP 和 IGRP 都是距离矢量路由协议，它们都定期地发送整个路由表到直接相邻的路由器。EIGRP 也属于距离矢量路由协议，但 EIGRP 是一个高级的距离矢量路由协议，同样具备很多链路状态路由协议的特征。

(1) 距离矢量路由协议路由环路的形成。执行距离矢量路由协议的路由器没有关于远端网络的确切信息, 以及对远端路由器的认识, 执行距离矢量路由协议的路由器获知网络的途径就是邻居路由器的路由表拷贝, 有时也称距离矢量路由协议为传闻路由协议, 道听途说, 不加以审核, 当然距离矢量路由协议也没有办法审核, 因为它们没有关于远端网络和路由器的确切消息, 这样极容易形成环路。

下面看一下在距离矢量路由协议中, 路由环路是如何形成的。这里以 RIP 路由协议为例, 在图 5-5-1 中, 路由器 A 把网络 1 的路由发给路由器 B, 路由器 B 学到了网络 1, 并把度量值标记为 1 跳, 即经过一台路由器可以到达, 下一跳路由器是 A; 路由器 B 把网络 1 的路由发给路由器 C 和路由器 E, 路由器 C 和路由器 E 都学到了网络 1, 并把度量值标记为 2 跳, 即经过两台路由器可以到达, 下一跳路由器是 B; 路由器 C 和路由器 E 都把网络 1 的路由发给路由器 D, 路由器 D 也学到了网络 1, 并把度量值标记为 3 跳, 即经过三台路由器可以到达, 下一跳路由器是 C 或 E, 即从两台路由器都可以到达, 路由器 D 去往网络 1 的数据将负载均衡。此时所有的路由器都拥有一致的认识和正确的路由表, 这时的网络被称为已收敛。

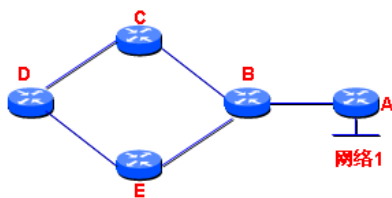


图 5-5-1 路由环路

路由器 B 也会把学到的网络 1 发给路由器 A, 路由器 A 发现网络 1 是直连路由, 有更小的管理距离 (直连的管理距离是 0, RIP 的管理距离是 120), 路由器 A 不会接收路由器 B 传过来的路由; 类似的, 路由器 C 也会把学到的网络 1 发给路由器 B, 路由器 B 发现从路由器 A 学到的网络 1 有 1 跳, 从路由器 C 学到的网络 1 有 3 跳, 路由器 B 不会接收路由器 C 传过来的网络 1 的路由; 类似的原理, 所有路由器都会学到正确的路由。

在网络 1 没有出现故障前, 路由器 D 有两条到达网络 1 的路径, 通过 C 或者 E 到达 B, 最后到达 A 所相连的网络 1。

① 当网络 1 断开时, 路由器 A 将网络 1 不可达的信息扩散到网络中 B, B 将网络 1 不可达的信息扩散到网络中 C 和 E, 此时 D 还不知道网络 1 出现故障不可以到达, 就在这个时候 D 发出了更新信息给 E, 认为通过 C 可以到达网络 1。当然这里也可能是 D 发出了更新信息给 C, 认为通过 E 可以到达网络 1, 这里以前面一种假设讨论。

- ② E 收到网络 1 又可以到达的信息 (通过 D 可以到达)。
- ③ E 更新自己的路由表并将网络 1 可到达的更新信息发送给 B。
- ④ B 更新自己的路由表并发送给 C 和 A。
- ⑤ C 更新自己的路由表并发送给 D, 此时路由环路产生。

(2) 距离矢量路由环路的解决办法。距离矢量路由协议环路的解决办法有 5 种:

- 最大跳计数 (maximum metric)

在上面的描述中, 尽管网络 1 出现了故障, 分组仍然在网络中循环。网络 1 的无效更新会不断地循环下去, 直到其他进程停止该循环。解决这个问题一个方法是定义最大跳计数。RIP 允许跳计数最大可以达到 15, 任何需要经过 16 跳到达的网络都被认为是不可达的。通过为无穷大指派一个最大值, 路由选择协议允许路由环路度量值超过其最大值之前继续存在。对于 RIP 路由协议来说, 当路由的跳数达到 16 前, 即使路由出现环路, 也保持路由条目的存在。超过 16 时, 不管网络有没有出现环路, 都认为路由不可达。最大跳计数其实并没有消除路由环路的存在, 只是把路由环路控制在一定的范围内。定义最大跳计数,

也限制了网络的规模，即使是合法的路由，也不能超过 16 跳。即使没有定义最大跳计数，当出现路由选择环路后，IP 分组也不会无限循环下去，因为 IP 分组中有一个 TTL 字段，主机传输分组前，TTL 字段会设置成 1~255 之间的一个整数值，该值独立于操作系统。路由器接收到分组后，会将 TTL 减 1，如果 TTL 变成 0，路由器将丢弃该 IP 分组，这样即使没有定义最大跳计数，IP 分组也不会在出现路由选择环路的网络中永远地传输下去。

- 水平分割 (split horizon)

另一个解决路由环路问题的方法被称为水平分割。具体做法就是限制路由器不能按接收信息的方向去发送信息。在图 5-5-1 中，路由器 C 和路由器 E 有关网络 1 的路由信息是从与路由器 B 相连的接口学到的，路由器 C 和路由器 E 将不会把网络 1 的信息从与路由器 B 相连的接口再传回去。这样路由器 D 最终会学到网络 1 故障的消息，所有路由器都会正确收敛，从而消除了路由环路。水平分割可以在简单的网络拓扑中消除路由环路，如果网络拓扑很复杂，规模很大，水平分割也不能消除路由环路。

- 路由中毒 (route poisoning)

路由中毒通过将故障网络的跳数设置成最大跳数加 1 来暗示网络的不可达。毒性反转 (poison reverse) 是避免路由环路的另一种方法，一旦从一个接口学到了一个路由，那么这个路由作为不可达路由从同一个接口回送。在图 5-5-1 中，路由器 A 上的网络 1 断开后，路由中毒使路由器 A 向路由器 B 宣告网络 1 的度量值为最大跳数加 1，针对 RIP 协议，就是 16 跳。路由器 B 收到路由器 A 的消息后，知道网络 1 有 16 跳，意味着网络 1 不可达，需要删除这条路径。毒性反转使路由器 B 向学到网络 1 路由的方向，即路由器 A 回送一个网络 1 不可达的消息。路由中毒或毒性反转用来克服大型网络路由选择环路。

如果没有采用路由中毒，发生拓扑变化的路由器，比如图 5-5-1 中的路由器 A，检测到直连路由网络 1 丢失，路由器 A 在发向路由器 B 的更新包中将不包含网络 1。偶尔一个更新包中没有包含网络 1，路由器 B 不会认为网络 1 已经失效，路由器 B 认为网络 1 仍然有效，并继续向路由器 C 和路由器 E 发送。当连续多个更新包中都没有包含网络 1 的信息时，路由器 B 才认为网络 1 失效，在 RIP 协议中，这个值默认是 180 秒，即连续的 6 个更新时间。类似的，路由器 C 和路由器 E 再过大概 180 秒才意识到网络 1 不可达，这样路由收敛的时间将会更长。如果采用路由中毒，路由器 A 向路由器 B 发送的更新包中包含网络 1 的跳数是 16，暗示网络 1 不可达。毒性反转则是路由器 B 反过来告诉路由器 A 网络 1 不可达。这里特别值得一提的是，毒性反转不受水平分割的影响。有关 RIP 相关的定时器，请参阅下一章的 6.1.3 节。

- 触发更新 (triggered update)

距离矢量路由协议一般是周期性发生路由更新的，比如 RIP 是 30 秒，更新周期未到，即使路由发生变化也不发送更新。而一般链路状态路由协议都是触发式更新，拓扑有变化时，马上发送路由更新。通过在距离矢量路由协议中使用触发更新，无须等待更新定时器期满就发送更新，这样更新很快就可传遍全网，减小出现路由环路的可能性。

- 抑制定时器 (holddown time)

可以用抑制定时器来避免计数到无穷大的问题。抑制定时器的使用分为下面 4 种情况：

① 如果一个路由器从邻居处接收到一条更新，指示以前可到达的网络目前不可达了，这个路由器标记该路由为不可达，同时启动一个抑制定时器，比如 RIP 默认是 180 秒。如果在抑制定时器期满以前，从同一个邻居处收到指示该网络又可达的更新，那么该路由器

标识这个网络可以到达，并且删除抑制定时器。

② 如果在抑制定时器期满以前，收到一个更新来自其他的邻居路由器，而且具有比以前路由更好的度量值，比如以前通过 RIP 学到某条路由的跳数是 3，现在收到的更新消息显示该路由的跳数是 2，那么该路由器标识这个网络可以到达，并删除抑制定时器。

③ 如果在抑制定时器期满以前，收到一个更新来自其他的邻居路由器，而且具有比以前路由相同或更差的度量值，比如以前通过 RIP 学到某条路由的跳数是 3，现在收到的更新消息显示该路由的跳数是 3 或 4，则忽略这个更新。

④ 在抑制定时器期满以后，删除抑制定时器，接收任何拥有合法度量值的更新。

2. 链路状态路由协议

链路状态路由协议也称为最短路径优先协议，链路状态路由协议使用的算法是最短路径优先（Shortest Path First, SPF）算法，有时也称 Dijkstras 算法。链路状态路由协议一般要维护 3 个表：一个是邻居表，用来跟踪直接连接的邻居路由器；一个是拓扑表，保存整个网络的拓扑信息数据库；还有一个是路由表，用来维护路由选择信息。链路状态路由器维护着远端路由器及其互连情况的全部信息，路由选择算法根据拓扑数据库执行 SPF 算法，链路状态路由选择协议不易出现路由环路问题。

表 5-5-3 对距离矢量路由协议和链路状态路由协议做了对比。

表 5-5-3 距离矢量路由协议与链路状态路由协议对比

	距离矢量路由协议	链路状态路由协议
配置和维护的技术要求	对管理员的要求不高	要求管理员的知识更全面
CPU、带宽和内存等资源要求	不需要大量的内存来存储信息，也不需要好的 CPU 来进行计算。如果路由表很大，周期性的更新会占用一定的带宽	需要大量的内存来存储邻居和拓扑信息，需要好的 CPU 来执行 SPF 算法。增量式更新，对带宽占用不多
收敛时间	采用周期性的更新，收敛时间较慢，有时甚至需要几分钟	触发式更新，收敛时间很快，一般几秒钟内就可完成
路由环路	慢速的收敛极易造成各路路由器的路由表不一致，很容易产生环路	基于全网的拓扑数据库，执行 SPF 算法，不易产生路由环路
扩展性	慢速的收敛和平面型的设计限制了网络的规模，不可能很大	快速的收敛和层次型的设计，网络的规模可以很大

5.5.5 常见的路由协议**

这里介绍几种常见的动态路由协议。

1. RIP

RIP（Routing Information Protocol，路由信息协议）是 Internet 中最古老的路由协议。RIP 采用距离矢量算法，即路由器根据距离选择路由，所以也称为距离向量协议。路由器收集所有可到达目的地的不同路径，并且保存有关到达每个目的地的最少站点数（hop）的路径信息，除到达目的地的最佳路径外，任何其他信息均予以丢弃。同时，路由器也把所收集的路由信息用 RIP 协议通知相邻的其他路由器。这样，正确的路由信息逐渐扩散到了全网。

RIP 简单，便于配置。但是 RIP 只适用于小型的网络，因为它允许的最大跳数为 15，任何超过 15 个站点的目的地均被标记为不可达。而且 RIP 每隔 30 秒一次的路由信息广播

也造成带宽的严重浪费，频繁的更新也影响路由器的性能。RIP 路由协议的收敛速度较慢，有时还会造成网络的环路。

本书第 6 章将介绍 RIP 协议。

2. OSPF

20 世纪 80 年代中期，RIP 已不能适应大规模异构网络的互连，OSPF (Open Shortest Path First, 开放式最短路径优先) 随之产生，它是 IETF (Internet Engineering Task Force, 互联网工程任务组) 的内部网关协议工作组为 IP 网络而开发的一种路由协议。

OSPF 是一种基于链路状态的路由协议，需要每个路由器向其同一管理域中的所有其他路由器发送链路状态通告信息。在 OSPF 的链路状态通告中包括接口信息、度量值和其他一些变量。运行 OSPF 的路由器首先必须收集所有的链路状态信息，并以本路由器为根，使用 SPF 算法算出到每个结点的最短路径。

本书第 8 章将介绍 OSPF 协议。

3. IS-IS

IS-IS (Intermediate System-to-Intermediate System, 中间系统到中间系统) 是 ISO 的标准协议，该协议与无连接网络服务 (Connectionless Network Service, CLNS) 和其他 ISO 路由协议一起使用。IS-IS 也是链路状态协议，采用 SPF 算法来计算到达每个网络的最佳路径。该协议在国内较少使用，在美国多见于运营商的网络，CCNA 考试中不包括 IS-IS。

4. IGRP

IGRP (Interior Gateway Routing Protocol, 内部网关路由协议) 也是一种距离矢量路由协议，它是思科公司私有的路由协议，使用复合的度量值 (包括延迟、带宽、负载和可靠性)。该路由协议较老，基本退出了历史舞台，也退出了 CCNA 考试的范畴。

5. EIGRP

EIGRP (Enhance IGREP, 增强的 IGRP) 是 IGRP 的升级版，也是思科公司私有的路由协议。EIGRP 结合了距离矢量和链路状态路由协议的优点，有更快的收敛，所使用的算法是 DUAL (Diffusing Update Algorithm, 弥散修正算法)。

本书第 7 章将介绍 EIGRP 协议。

6. BGP

前面介绍的 5 种协议都是 IGP 协议，BGP 是为 TCP/IP 互联网设计的 EGP，用于多个自治系统之间。它既不是纯粹的链路状态算法，也不是纯粹的距离矢量算法，各个自治系统可以运行不同的内部网关协议，不同的自治系统通过 BGP 交换网络可达信息。BGP 是 CCNP 中的内容，CCNA 中不要求掌握。

【快问快答】在图 5-5-2 中，R1 可以 ping 通 PC2，PC1 却 ping 不通 PC2，所有设备的 IP 地址配置都正确，所有的接口都正常。出现上述现象的可能原因是什么？

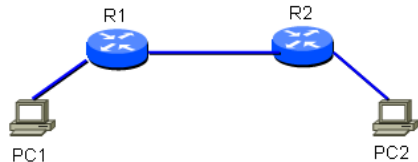


图 5-5-2 静态路由排错

答：R1 可以 ping 通 PC2，说明 R1 上添加了去往 PC2 所在网段的静态路由。下面分析 PC1 不能 ping 通 PC2 的原因：PC1 把去往 PC2 的包发往自己的网关，

R1 上已经有去往 PC2 所在网段的静态路由了, R1 查询路由表, 把包转发给 R2, R2 查询路由表, 把包转发给 PC2, 数据包正常到达了 PC2。PC2 知道是 PC1 发过来的 ping 包, PC2 进行应答, 把包发给 PC2 的网关, 也就是 R2, R2 查询自己的路由表, 假如 R2 有去往 PC1 所在网段的静态路由, R2 把包发给 R1, R1 再把包发给 PC1, 结果是 PC1 可以 ping 通 PC2, 可事实是 ping 不通, 这只能说明前面的假设有错误, 即 R2 上没有去往 PC1 所在网段的静态路由。

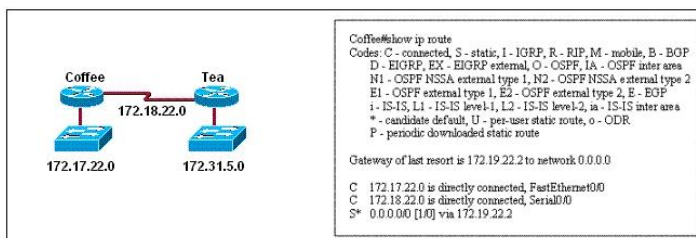


5.6 真题精选***

1. What functions do routers perform in a network? (Choose two.)

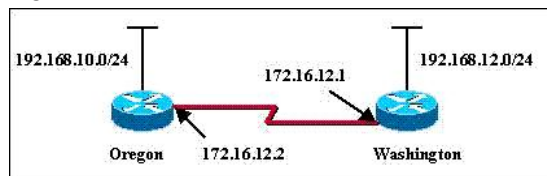
- A. packet switching
- B. access layer security
- C. path selection
- D. VLAN membership assignment
- E. bridging between LAN segments
- F. microsegmentation of broadcast domains

2. Users on the 172.17.22.0 network cannot reach the server located on the 172.31.5.0 network. The network administrator connected to router Coffee via the console port, issued the show ip route command, and was able to ping the server. Based on the output of the show ip route command and the topology shown in the graphic, what is the cause of the failure?



- A. The network has not fully converged.
- B. IP routing is not enabled.
- C. A static route is configured incorrectly.
- D. The FastEthernet interface on Coffee is disabled.
- E. The neighbor relationship table is not correctly updated.
- F. The routing table on Coffee has not updated.

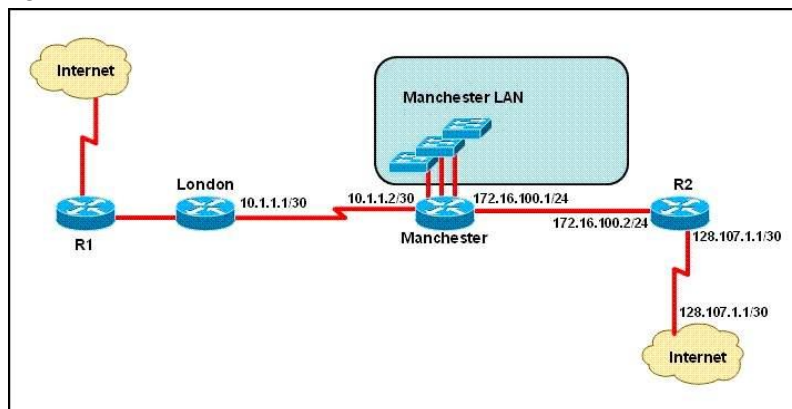
3. The network administrator of the Oregon router adds the following command to the router configuration: ip route 192.168.12.0 255.255.255.0 172.16.12.1. What are the results of adding this command? (Choose two.)



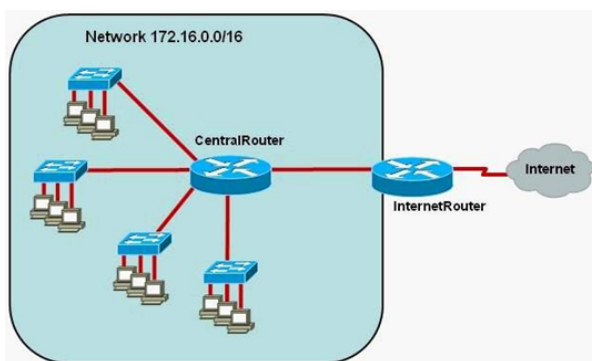
- A. The command establishes a static route.
- B. The command invokes a dynamic routing protocol for 192.168.12.0.

- C. Traffic for network 192.168.12.0 is forwarded to 172.16.12.1.
- D. Traffic for all networks is forwarded to 172.16.12.1.
- E. This route is automatically propagated throughout the entire network.
- F. Traffic for network 172.16.12.0 is forwarded to the 192.168.12.0 network.

4. Refer to the exhibit. The speed of all serial links is E1 and the speed of all Ethernet links is 100 Mb/s. A static route will be established on the Manchester router to direct traffic toward the Internet over the most direct path available. What configuration on the Manchester router will establish a route toward the Internet for traffic that originates from workstations on the Manchester LAN?

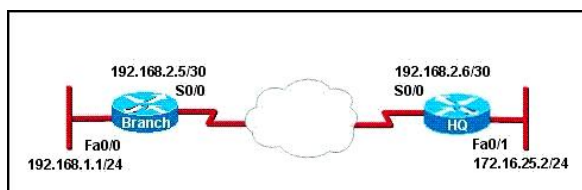


- A. `ip route 0.0.0.0 255.255.255.0 172.16.100.2`
 - B. `ip route 0.0.0.0 0.0.0.0 128.107.1.1`
 - C. `ip route 0.0.0.0 255.255.255.252 128.107.1.1`
 - D. `ip route 0.0.0.0 0.0.0.0 172.16.100.1`
 - E. `ip route 0.0.0.0 0.0.0.0 172.16.100.2`
 - F. `ip route 0.0.0.0 255.255.255.255 172.16.100.2`
5. Which two statements are true about the command `ip route 172.16.3.0 255.255.255.0 192.168.2.4`? (Choose two.)
- A. It establishes a static route to the 172.16.3.0 network.
 - B. It establishes a static route to the 192.168.2.0 network.
 - C. It configures the router to send any traffic for an unknown destination to the 172.16.3.0 network.
 - D. It configures the router to send any traffic for an unknown destination out the interface with the address 192.168.2.4.
 - E. It uses the default administrative distance.
 - F. It is a route that would be used last if other routes to the same destination exist.
6. Refer to the exhibit. The network administrator requires easy configuration options and minimal routing protocol traffic. What two options provide adequate routing table information for traffic that passes between the two routers and satisfy the requests of the network administrator? (Choose two.)



- A. a dynamic routing protocol on InternetRouter to advertise all routes to CentralRouter.
- B. a dynamic routing protocol on InternetRouter to advertise summarized routes to CentralRouter.
- C. a static route on InternetRouter to direct traffic that is destined for 172.16.0.0/16 to CentralRouter.
- D. a dynamic routing protocol on CentralRouter to advertise all routes to InternetRouter.
- E. a dynamic routing protocol on CentralRouter to advertise summarized routes to InternetRouter.
- F. a static, default route on CentralRouter that directs traffic to InternetRouter.

7. Refer to the exhibit. A network associate has configured the internetwork that is shown in the exhibit, but has failed to configure routing properly. Which configuration will allow the hosts on the Branch LAN to access resources on the HQ LAN with the least impact on router processing and WAN bandwidth?



- A. HQ(config)# ip route 192.168.1.0 255.255.255.0 192.168.2.5
Branch(config)# ip route 172.16.25.0 255.255.255.0 192.168.2.6
- B. HQ(config)# router rip
HQ(config-router)# network 192.168.2.0
HQ(config-router)# network 172.16.0.0
Branch(config)# router rip
Branch (config-router)# network 192.168.1.0
Branch (config-router)# network 192.168.2.0
- C. HQ(config)# router eigrp 56
HQ(config-router)# network 192.168.2.4
HQ(config-router)# network 172.16.25.0
Branch(config)# router eigrp 56

Branch(config-router)# network 192.168.1.0

Branch(config-router)# network 192.168.2.4

D. HQ(config)# router ospf 1

HQ(config-router)# network 192.168.2.4 0.0.0.3 area 0

HQ(config-router)# network 172.16.25.0 0.0.0.255 area 0

Branch(config)# router ospf 1

Branch(config-router)# network 192.168.1.0 0.0.0.255 area 0

Branch(config-router)# network 192.168.2.4 0.0.0.3 area 0

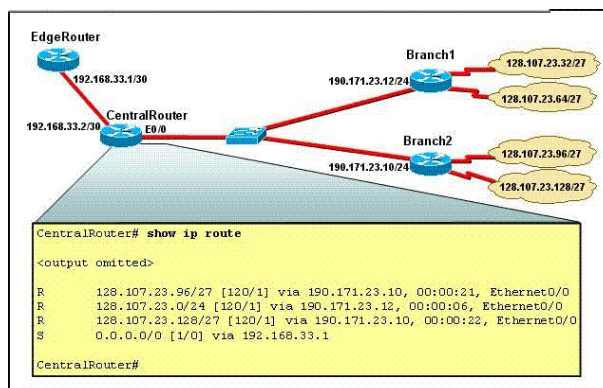
8. A router learns about a remote network from EIGRP, OSPF, and a static route. Assuming all routing protocols are using their default administrative distance, which route will the router use to forward data to the remote network?

- A. The router will use the static route.
- B. The router will use the OSPF route.
- C. The router will use the EIGRP route.
- D. The router will load balance and use all three routes.

9. A router receives information about network 192.168.10.0/24 from multiple sources. What will the router consider the most reliable information about the path to that network?

- A. a directly connected interface with an address of 192.168.10.254/24
- B. a static route to network 192.168.10.0/24
- C. a RIP update for network 192.168.10.0/24
- D. an OSPF update for network 192.168.0.0/16
- E. a default route with a next hop address of 192.168.10.1
- F. a static route to network 192.168.10.0/24 with a local serial interface configured as the next hop.

10. Refer to the exhibit. RIPv2 is in use on the network with no standard policy in place for summarization. A packet arrives at CentralRouter with a destination IP address of 208.149.23.91. Given the output that is shown, how will CentralRouter process that packet?



- A. It will forward the packet to 190.171.23.10.
- B. It will forward the packet to 190.171.23.12.

- C. It will forward the packet to 192.168.33.1.
- D. It will hold the packet for 22 seconds.
- E. It will hold the packet for 21 seconds.
- F. It will discard the packet because there is no matching route.

11. What are two drawbacks of implementing a link-state routing protocol?
(Choose two.)

- A. the sequencing and acknowledgment of link-state packets
- B. the requirement for a hierarchical IP addressing scheme for optimal functionality
- C. the high volume of link-state advertisements in a converged network
- D. the high demand on router resources to run the link-state routing algorithm
- E. the large size of the topology table listing all advertised routes in the converged network



5.7 真题解答***

1. 解：AC

题目问：路由器在网络中的功能是什么？路由器在网络中的两个主要功能是包交换和路径选择，当路由器从一个接口收到数据包后，路由器将查询路由表，进行路径选择，找到外出接口，然后把数据包交换到外出接口，故 AC 正确。B 选项提到的访问层安全是由交换机实现的；D 选项提到的 VLAN 成员分配也是由交换机完成的；E 选项提到的在局域网分段间进行桥接，是由交换机或网桥完成的；F 选项提到可以微分广播域，路由器可以隔离广播域，路由器的每一个接口就是一个广播域，但路由器的接口数量一般都很少，说成微分有点不太合适。

2. 解：C

题目问：172.17.22.0 网段的用户不能访问 172.31.5.0 网段的服务器，网络管理员通过 Console 端口连接到 Coffee 路由器，执行 show ip route 命令并能够 ping 通那台服务器，命令的输出如图所示，根据图中 show ip route 命令的输出，可能是什么原因导致了 172.17.22.0 网段的用户不能访问 172.31.5.0 网段的服务器？这道题出得很好，有相当的难度。但题本身有错误，判断的依据一是：考生注意路由表输出中的“S* 0.0.0.0 [1/0] via 172.19.22.2”，这里显示的是一条默认路由，默认路由的下一跳是 172.19.22.2，路由器的路由表中并没有去往 172.19.22.2 的路由条目，这条默认路由将不会出现在路由器的路由表中，输出中的 172.19.22.2 改成 172.18.22.2 就正确了；判断的依据二是：如果 Coffee 路由器上的默认路由配置错误，Coffee 路由器也 ping 不通 172.31.5.0 网段的服务器，可题目中却说可以 ping 通，再次确认题目有错，输出中的 172.19.22.2 改成 172.18.22.2 就正确了。接下来使用排除法进行选择：A 选项说网络没有完全收敛，图中使用的是静态路由，不是动态路由，不存在路由完全收敛的问题；B 选项说没有启用 IP 路由协议，如果没有启用 IP 路由协议，Coffee 路由器的路由表中将不会出现路由条目；C 选项说静态路由配置得不正确，这种可能是存在的，假如题目没有出错，Coffee 路由器的路由表中出现的将是“S* 0.0.0.0 [1/0] via 172.18.22.2”，Coffee 路由器能够 ping 通 172.31.5.0 网段的服务器，但 Tea 路由器上没有配置 172.17.22.0 的静态路由，将导致 172.17.22.0 网段的用户不能访问 172.31.5.0 网段的服务器；D 选项说 Coffee 路由器的快速以太网接口被禁用，如果接口被禁用，路由表中将不会出现“C

172.18.22.0...” 的路由条目；E 选项说邻居关系表没有正确更新，静态路由中不存在邻居关系表更新；F 选项说 Coffee 路由器的路由表没有更新，静态路由不需要更新。综上所述，正确的答案应该是 C。

3. 解：AC

题目问：根据图，Oregon 路由器的管理员给路由器添加下面的配置“ip route 192.168.12.0 255.255.255.0 172.16.12.1”，增加这条命令的结果是什么？这条命令配置的是一条简单静态路由，正确答案是 A 和 C。

4. 解：E

题目问：参照图，所有的串行线路都是 E1（2.048Mb/s），所有的以太网都是 100Mb/s。一条静态路由将被配置在曼彻斯特路由器上，来转发多数直连网段的流量到 Internet，在曼彻斯特路由器上的什么配置将建立一条路由，转发曼彻斯特局域网的流量到 Internet？这里考的是默认路由，只需配置一条默认路由就可以了，默认路由是静态路由中特殊的一种，正确答案是 E。如果还有一个选项是“ip route 0.0.0.0 0.0.0.0 10.1.1.1”，这里仍然选择 E，因为曼彻斯特从 R2 连接到 Internet 更合理，如果从一条慢速的链路连接到伦敦路由器，然后再接入 Internet，就显得不合理。

5. 解：AE

题目问：关于这条命令“ip route 172.16.3.0 255.255.255.0 192.168.2.4”，哪两个语句的叙述是正确的？该命令配置的是去往 172.16.3.0/24 的静态路由，没有在静态路由的最后添加管理距离参数，使用的就是默认的管理距离，静态路由默认的管理距离是 1。故正确的答案是 A 和 E。

6. 解 CF

题目问：网络管理员要求容易配置和最小化路由协议的流量，哪两个选项提供了在两台路由器间传输的足够路由信息，并且能够满足网络管理员的要求？静态路由不需要传输路由协议的流量，可以最小化地占用带宽资源。因为在这个图中，InternetRouter 要访问内网 172.16.0.0/16 只能通过路由器 CentralRouter，所以需要在 InternetRouter 上配置一条通过 CentralRouter 到达 172.16.0.0/16 网段的静态路由。同样，内网要访问 Internet，也只能通过路由器 InternetRouter 才能到达，需要在 CentralRouter 上配置一条默认路由到 Internet。

7. 解：A

题目问：一个网络助手配置了图中的网络，但没有配置正确的路由，哪种配置将允许 Branch 路由器上的局域网访问 HQ 路由器上的局域网？要求要最少占用路由器资源的广域网的带宽。动态路由协议都是需要发送更新包来传递路由的，而这些都会占用带宽，有些路由协议还需要占用 CPU 和内存来执行路由协议算法。为了减少资源和带宽的占用可以采用静态路由，不会占用任何带宽，也不需要占用 CPU 和内存来执行路由算法。

8. 解：A

题目问：一台路由器通过 EIGRP、OSPF 和静态路由都学到了一个远程网络。假设所有的路由协议都使用默认的管理距离，路由器将使用哪种路由转发数据到远程网络？这道题考的是路由选路，对于相同的路由条目，管理距离越小可信度越高，静态的默认管理距离

是 1, EIGRP 的是 90, OSPF 的是 110。综上所述, 正确的答案应该是 A。

9. 解: A

题目问: 一台路由器从多处收到关于网络 192.168.10.0/24 的路由, 这台路由器将认为哪条路径是去往这个网络的最可信路径? 当到达同一个目的地有多种路径选择的时候, 根据 5.5.3 节叙述的选路原则, 首先根据最长匹配原则: A、B、C 和 F 都是 24 位匹配, D 是 16 位匹配, E 是 0 位匹配; 其次根据管理距离, 管理距离小的路由的可信度高: A 是直连路由, 管理距离是 0; B 是静态路由, 管理距离是 1; C 是 RIP 路由, 管理距离是 120; F 是静态路由, 但使用的是本地的外出接口, 管理距离也是 0, 直连路由和使用外出接口的静态路由的管理距离都是 0, 两者都存在时, 直连路由优先。综上所述, A 是正确答案。

10. 解: B

题目问: 网络中使用 RIPv2, 没有使用自动汇总, 一个目的 IP 地址是 208.149.23.91 (题目有错, 应该是 128.107.23.91) 的数据包到达 CentralRouter 路由器, 根据图中显示的路由表, CentralRouter 路由器如何处理这个数据包? 本题虽然提到 RIPv2 和自动汇总 (本书后面会介绍到), 但最主要考的还是路由选路, 路由表中有 4 个条目, 128.107.23.91 不属于 128.107.23.96/27 子网, 也不属于 128.107.23.128/27 子网, 但属于 128.107.23.0/24 子网和 0.0.0.0/0 子网, 根据选路原则的第一条——最长匹配优先, 该数据包将被发往 190.171.23.12。

11. 解: BD

题目问: 执行链路状态路由协议的两个缺点是什么? 链路状态路由协议执行链路状态路由算法时, 需要占用大量的内存和 CPU 资源。此外, 链路状态路由协议的路由汇聚只能发生在区域的边界, 这就要求链路状态路由协议要有一个层次型的 IP 地址架构。综上所述, 正确的答案是 B 和 D。

第 6 章

RIP***

本章介绍 RIP 的主要特征、RIP 定时器的使用、RIPv1 的配置、VLSM 和 CIDR 的作用、RIPv1 的局限性、RIPv2 的配置、路由查找过程等。



6.1 RIP 概述***

RIP (Routing Information Protocol, 路由信息协议) 是应用较早、使用较普遍的内部网关协议 (Interior Gateway Protocol, IGP), 适用于小型同类网络, 是典型的距离矢量 (distance-vector) 路由协议, 文档见 RFC1058、RFC1723。RIP 协议是一个国际标准, 经受了长期的实际运行考验, 在网络界已被广为运用, 所有的路由器厂商都支持它, 而且 RIP 在各种操作系统中都能很容易地进行配置和故障排除。在那些没有冗余链路的网络中 RIP 能很好地进行工作, 但 RIP 的最大缺点在于它无法在具有冗余链路的网络中有效地运用。所以对于大型网络或需要具备冗余链路的网络, 就必须考虑采用其他路由协议了。

6.1.1 RIP 主要特征***

RIP 协议的默认管理距离是 120, 处于 UDP 协议的上层, RIP 所接收的路由信息都封装在 UDP 协议的数据报中, RIP 使用 UDP 520 端口发送和接收路由信息, 先更新本地的路由表, 然后再通知其他路由器。

RIP 作为距离矢量路由协议的典型代表, 具有以下主要特征:

(1) 使用 Hop count (跳计数) 作为路径选择的度量值

一个报文从本结点到目的结点, 中途经历的中转次数或路由器的数量被称为跳计数, RIP 采用距离向量算法, 它通过比较到达目的站点的各个路由的 Hop count, 即跳数的大小, 从中选择具有最小跳数的路由作为最佳路由。RIP 只保留到目的地的最佳路由, 当交换过来的新的路由信息提供了一条更佳的路由时, RIP 就用它来替换旧的信息。

RIP 在选择路由时不考虑链路的带宽, 而仅仅用 Hop count 作为衡量路径好坏的唯一标准。这就造成了在一个实际的网络中, 采用快速以太网 (100Mb/s) 连接的链路可能仅仅因为比 10Mb/s 以太网链路多出 1 个 Hop, 致使 RIP 认为 10Mb/s 链路是一条更优化的路由, 而实际上却并非如此。

(2) 最大跳数 15

如果一个网络的跳计数大于 15, 则认为该网络失效。这就是说, 一条路由的 Hop count 值达到 16 后, RIP 认为这条路由无效。显然, 这样的定义有效地预防了环路的蔓延, 对于小网络高效易行; 但是对于超过 15 个 Hop 的大型网络来说, RIP 就有局限性。

(3) 周期性的广播或多点传送整个路由表

RIP 版本 1 采用的是广播式更新，网络中的所有设备都会受到更新的影响。RIP 版本 2 采用的是组播更新，没有运行 RIP 版本 2 的网络设备不受影响。不管是广播式更新还是组播式更新，即使网络拓扑没有发生变化，RIP 也会周期性地（默认是 30 秒）发送整个路由表给相邻路由器。

6.1.2 RIP 拓扑变化**

拓扑发生变化时，RIP 路由的处理过程如图 6-1-1 所示。

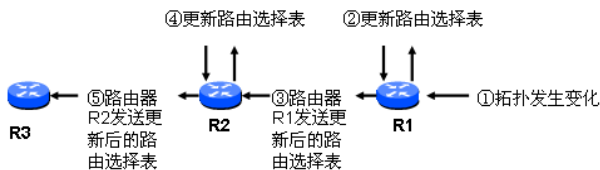


图 6-1-1 RIP 拓扑变化

- ① 路由器 R1 的拓扑发生变化。
- ② 路由器 R1 更新自己的路由表。
- ③ 路由器 R1 发送更新后的整个路由表给相邻路由器 R2。
- ④ 路由器 R2 更新自己的路由表。
- ⑤ 路由器 R2 发送更新后的整个路由表给相邻路由器 R3。

从上面的更新过程中可以发现，每台路由器得知网络拓扑发生变化时，都是先更新本地的路由表，再发送更新后的路由表。

接下来看一下运行 RIP 协议的路由器间是如何相互学习的。在 RIP 协议运行前，图 6-1-2 中的路由器 R1、R2、R3 上只有相关的直连路由信息。

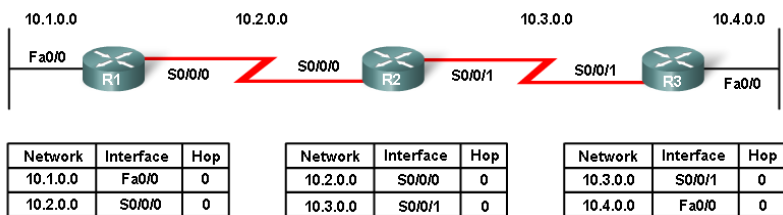


图 6-1-2 RIP 运行前

- ① 运行 RIP 路由协议，路由器 R1、R2、R3 各自宣告自己直连的网络。
- ② 假设 R1 首先发送路由更新，R1 把自己直连的网络 10.1.0.0 和 10.2.0.0 以 1 跳的度量值告诉 R2。
- ③ R2 收到 R1 的路由表后，R2 把自己的路由表和 R1 传过来的路由表进行对比，R2 发现自己的路由表中没有 10.1.0.0，R2 记下这条路由及对应的路由器接口和跳数 1；R2 发现自己的路由表中已经有 10.2.0.0，并且还是直连路由，直连路由的管理距离是 0，学到的 RIP 路由的管理距离是 120，直连路由更好，R2 忽略 R1 传过来的 10.2.0.0。
- ④ R2 把自己路由表中直连的网络 10.2.0.0 和 10.3.0.0 以 1 跳的度量值告诉 R3；R2 把自己路由表中学到的 RIP 网络 10.1.0.0 以 2 跳的度量值告诉 R3。

⑤ R3 收到 R2 的路由表后, R3 把自己的路由表和 R2 传过来的路由表进行对比, R3 发现自己的路由表中没有 10.1.0.0, R3 记下这条路由及对应的路由器接口和跳数 2; R3 发现自己的路由表中没有 10.2.0.0, R3 记下这条路由及对应的路由器接口和跳数 1; R3 发现自己的路由表中已经有 10.3.0.0, 并且还是直连路由, R3 忽略 R2 传过来的 10.3.0.0。这样路由器 R3 就学到了完整的路由条目。

⑥ 类似地, 路由器 R3 也会把自己的路由表发送给 R2, R2 也会发送给 R1, 最后所有的路由器都可以学到所有的网络。每个路由器最后的路由表如图 6-1-3 所示。

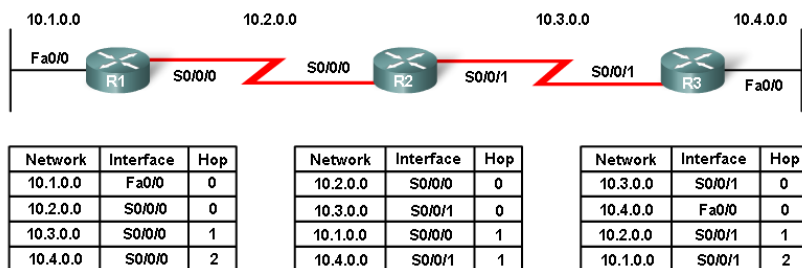


图 6-1-3 RIP 运行后

6.1.3 RIP 定时器***

RIP 使用 4 种不同类型的定时器来管理它的性能。在运行 RIP 协议的路由器上使用“show ip protocols”命令, 显示如下:

```
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 0 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
```

(1) **路由更新定时器**: 用于设置定期路由更新的时间间隔, 默认是 30 秒。在上面的输出中, “Sending updates every 30 seconds” 指的就是路由更新定时器, 每隔 30 秒路由器会把自己的整个路由表完整地拷贝给相邻的路由器, 即使本路由器的拓扑没有发生变化也会拷贝。

(2) **路由失效定时器**: 路由器在认定一个路由为无效路由之前所需要等待的时间, 默认是 180 秒。在上面的输出中, “Invalid after 180 seconds” 指的就是失效定时器。如果路由器在这个期间内没有收到关于某个路由的更新消息, 它将认为这个路由失效。当这一情况发生时, 路由器将给它所有相邻的路由器发送一个更新消息, 以通知它们这个路由已经无效。

(3) **抑制定时器 (holddown time)**: 用于设置路由信息被抑制的时间。当收到指示某个路由为不可达的更新数据包时, 路由器将会进入 holddown time, 默认也是 180 秒, 即上面输出中的 “hold down 180”。有关抑制定时器, 请参阅第 5 章的 5.5.4 节。

(4) **路由刷新定时器**: 用于设置某个路由成为无效路由, 并将它从路由表中删除的时间间隔, 默认是 240 秒, 即上面输出中的 “flushed after 240”。在将它从路由表中删除之前, 路由器会通告它的邻居这个路由即将消亡。路由失效定时器的值必须小于路由刷新定时器的值, 这就为路由器提供了足够的时间, 用来在本地路由表更新前通告它的邻居有关这一无效路由的情况。

在不考虑使用任何防止距离矢量协议路由选择环路的情况下，可以这样来理解上面的 4 种定时器。结合图 5-5-1，在默认情况下 RIP 每 30 秒发送一次路由更新，如果某个拓扑发生变化，这里是路由器 A 上的网络 1 失效，路由器 A 发往路由器 B 的更新包中不再包含网络 1，路由失效定时器、路由抑制定时器和路由刷新定时器同时开始启动，连续 6 个更新周期，路由器 B 都没有收到路由器 A 发过来的网络 1 的信息，路由器 B 认为网络 1 失效。这里用到的是路由失效定时器，路由失效之前，如果路由器 B 收到发往网络 1 的数据包，路由器 B 是往路由器 A 上进行转发的。在路由器 B 上网络 1 失效前的 180 秒内，路由器 B 上的网络 1 处在抑制状态。接下来的 60（路由刷新定时器 240—路由抑制定时器或路由失效定时器 180）秒内，虽然路由器 B 的路由表中仍有网络 1 的条目，但路由器 B 认为网络 1 可能 down 掉（possibly down），路由器 B 不再转发去往网络 1 的数据包，60 秒过后，路由器 B 从路由表中删除网络 1 的信息。



6.2 RIP 配置**

RIPv1 是一个有类的距离矢量路由选择协议，不支持 VLSM（Variable Length Subnet Masking，变长子网掩码）和 CIDR（Classless Inter-Domain Routing，无类域间路由）。有关 VLSM 和 CIDR 将在下一节进行讨论。

本节介绍 RIP 的基本配置，包括：一般配置、查看路由表、负载均衡、查看路由协议、水平分割、触发更新、单播更新、默认路由、浮动静态路由等，很多配置同样适用于 RIPv2。

1. 基本配置

这里使用 RIP 完成如图 5-2-1 所示的网络互连。路由器 R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#no cdp run
关闭 CDP 协议，目的是关闭模拟器中以太网端口双工不匹配的提示信息，避免受提示信息的干扰。
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int fa 0/0
R1(config-if)#ip add 13.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#router rip
配置 RIP 协议，启动路由选择进程。
R1(config-router)#network 1.0.0.0
network 命令是需要的，因为它允许路由选择进程决定哪些接口将参与发送和接收路由选择更新信息。
network 命令能在路由器上所有位于特定网络内的接口上启动路由选择协议，network 命令也使得路由
器将该网络发布出去。宣告 Loopback 接口的直连网络，RIP 在配置网络地址时使用的是有类地址，即
使配置的是 1.1.1.0，哪怕是 1.1.1.1，使用 show running-config 命令查看配置时，发现配置都
自动被改成了 1.0.0.0，如果路由器有多个接口属于 1.0.0.0 这个 A 类网络，并不需要 network
1.0.0.0 多次，一次就够了。
R1(config-router)#net 12.0.0.0
宣告 S1/1 接口的直连网络。
R1(config-router)#net 13.0.0.0
宣告 Fa0/0 接口的直连网络。
```

路由器 R2 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
```

```

R2(config)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int lo0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
R2(config-if)#router rip
R2(config-router)#net 2.0.0.0
R2(config-router)#net 12.0.0.0
R2(config-router)#net 23.0.0.0

```

路由器 R3 的配置如下：

```

Router>en
Router#conf t
Router(config)#host R3
R3(config)#no cdp run
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int fa 0/0
R3(config-if)#ip add 13.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#router rip
R3(config-router)#net 3.0.0.0
R3(config-router)#net 13.0.0.0
R3(config-router)#net 23.0.0.0

```

2. 配置动态路由的一般步骤

在路由器 R1、R2 或 R3 上任意 ping 图 5-2-1 中标出的 IP 地址，发现均可 ping 通。这里总结一下配置动态路由的一般步骤。

步骤 1：为路由器每个接口配置 IP 地址。

步骤 2：确定本路由器有哪些直连网段。

步骤 3：在路由进程中宣告所有的直连网络。

步骤 4：配置动态路由中的其他可选信息。

从上面的配置和总结中，读者可能并没有发现动态路由选择协议在配置上的方便性，试想一下有 100 台路由器，101 个网络，每个路由器上有两个直连网络的情况，如果是配置静态路由，每台路由器上需要添加 99 个静态路由条目，而动态路由协议只需宣告两个直连的路由就可以了，即使网络中再多出 100 台路由器，已有动态路由器的配置几乎不变，每台路由器仍然是加入自己的直连网络。静态路由协议要考虑的是所有非直连网络，需要纵观整个网络的路由分布；动态路由协议要考虑的是自己的直连网络，不用纵观整个网络的路由分布。

3. 查看路由表

在路由器 R1 上使用“show ip route”命令，查看路由器 R1 的路由表，显示如下：

```

R1#show ip route
{Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route

```

o - ODR, P - periodic downloaded static route
为了节省篇幅，以后除非有特殊需要，否则“show ip route”命令的输出都不再包括括号中的部分。

```
Gateway of last resort is not set
}
  1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, Loopback0
R    2.0.0.0/8 [120/1] via 12.1.1.2, 00:00:10, Serial1/1
R    3.0.0.0/8 [120/1] via 13.1.1.3, 00:00:21, FastEthernet0/0
R    23.0.0.0/8 [120/1] via 13.1.1.3, 00:00:21, FastEthernet0/0
    [120/1] via 12.1.1.2, 00:00:10, Serial1/1
  12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/1
  13.0.0.0/24 is subnetted, 1 subnets
C    13.1.1.0 is directly connected, FastEthernet0/0
```

从上面的输出中可以看到，路由器 R1 上拥有全网所有的路由（6 条），路由条目最前面的字母表示路由的代码，与 CCNA 相关的有：“C”表示路由器直连路由，“S”表示管理员静态配置的路由，“R”表示通过 RIP 学到的路由，“D”表示通过 EIGRP 学到的路由，“O”表示通过 OSPF 学到的路由。

“R 2.0.0.0/8 [120/1] via 12.1.1.2, 00:00:10, Serial1/1”中的 R 表示通过 RIP 学来的路由；2.0.0.0/8 是学到的远程网络，因为 RIP 是一个有类路由协议，且自动进行汇总，2.2.2.0/24 被自动汇总成 2.0.0.0/8；[120/1]中 120 表示的是 RIP 的管理距离，1 表示的是 RIP 的跳数，从路由器 R1 到达 2.0.0.0/8 需要一跳，即经过一台路由器可以到达；“via 12.1.1.2”，R1 去往 2.0.0.0/8 的下一跳路由器直连接口的 IP 地址是 12.1.1.2；“00:00:10”，是收到最后一次路由更新的时间；“Serial1/1”，是本路由器的去往 2.0.0.0/8 路由的外出接口。

断开路由器 R1 和 R2 之间的链路：

```
R1(config)#int s1/1
R1(config-if)#shut
```

稍等一会，等路由收敛后，在路由器 R1 上使用“show ip route”命令，查看路由器 R1 的路由表，显示如下：

```
R1#show ip route
  1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, Loopback0
R    2.0.0.0/8 [120/2] via 13.1.1.3, 00:00:21, FastEthernet0/0
R    3.0.0.0/8 [120/1] via 13.1.1.3, 00:00:21, FastEthernet0/0
R    23.0.0.0/8 [120/1] via 13.1.1.3, 00:00:21, FastEthernet0/0
  13.0.0.0/24 is subnetted, 1 subnets
C    13.1.1.0 is directly connected, FastEthernet0/0
```

从上面的输出中可以看出，RIP 可以根据网络拓扑动态调整路由表，这是所有动态路由协议的特点，也是与静态路由相比，动态路由协议的一个优点。关闭 R1 和 R2 之间的直连链路，导致 R1 和 R2 之间的路由消失，R1 的路由表中只有 5 条路由：2 条直连路由，3 条 RIP 路由，所有的远程网络都是通过路由器 R3 学到的。实验完成后，重新打开路由器 R1 的 S1/1 接口。

4. 负载均衡

```
R    23.0.0.0/8 [120/1] via 13.1.1.3, 00:00:21, FastEthernet0/0
    [120/1] via 12.1.1.2, 00:00:10, Serial1/1
```

前面的输出表示路由器 R1 去往 23.0.0.0/8 路由有两个下一跳，即通过 R3 和 R2 都可以到达，R1 去往 23.0.0.0 的包将被负载均衡到路由器 R2 和 R3。从这里可以看出，RIP 仅使

用跳数作为度量值，而不考虑链路的带宽。本例中，R1 和 R3 之间是 100Mb/s 链路，R1 和 R2 之间的链路只有 1.544Mb/s，RIP 在执行路由选路时，仅考虑跳数，忽略链路的实际带宽。

RIP 默认支持 4 条路径的负载均衡，最大可支持 6 条，通过使用下面的命令设置：

```
R1(config)#router rip
R1(config-router)#maximum-paths 6
```

在路由器 R1 上执行“debug ip icmp”命令，然后 ping 23.1.1.2，结果显示如下：

```
R1#debug ip icmp
ICMP packet debugging is on
R1#ping 23.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/30/76 ms
R1#
*Mar 1 01:14:16.267: ICMP: echo reply rcvd, src 23.1.1.2, dst 13.1.1.1
*Mar 1 01:14:16.287: ICMP: echo reply rcvd, src 23.1.1.2, dst 13.1.1.1
*Mar 1 01:14:16.315: ICMP: echo reply rcvd, src 23.1.1.2, dst 13.1.1.1
*Mar 1 01:14:16.319: ICMP: echo reply rcvd, src 23.1.1.2, dst 13.1.1.1
*Mar 1 01:14:16.343: ICMP: echo reply rcvd, src 23.1.1.2, dst 13.1.1.1
```

从上面的输出中看到的结果却是去往 23.1.1.2 的数据包全部是从 R3 走的（从返回的地址是 13.1.1.1 可以得出这个结论），并没有执行负载均衡。原因是这样的，当进行 IP 路由选择时，思科 IOS 软件提供两种负载均衡的方法：

- 基于每个分组的负载均衡，称为进程交换。
- 基于每个目的的负载均衡，称为快速交换。

如果启用进程交换，路由器将基于每个分组交替使用路径，即第一个分组使用第一条路径，第二个分组使用第二条路径，第三个分组再使用第一条路径，有多条负载均衡路径的执行与此类似。如果启用快速交换，那么只有一条到达目的地址的路径会被缓存，到达指定地址的所有分组都使用相同的路径。使用 no ip cef 关闭快速交换，使用进程交换，再次测试，显示如下：

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no ip cef
R1(config)#do ping 23.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/32/52 ms
R1(config)#
*Mar 1 01:30:56.311: ICMP: echo reply rcvd, src 23.1.1.2, dst 12.1.1.1
*Mar 1 01:30:56.363: ICMP: echo reply rcvd, src 23.1.1.2, dst 13.1.1.1
*Mar 1 01:30:56.391: ICMP: echo reply rcvd, src 23.1.1.2, dst 12.1.1.1
*Mar 1 01:30:56.395: ICMP: echo reply rcvd, src 23.1.1.2, dst 13.1.1.1
*Mar 1 01:30:56.439: ICMP: echo reply rcvd, src 23.1.1.2, dst 12.1.1.1
```

从上面的输出中可以看出，R1 去往 23.1.1.2 的数据包执行了负载均衡（从返回的地址分别是 13.1.1.1 和 12.1.1.1 可以得出这个结论）。

5. 查看路由协议

在路由器 R1 上使用“show ip protocols”命令，查看路由器 R1 上运行的路由协议，显示如下：

```
R1#show ip protocols
```

```

Routing Protocol is "rip"                                ①
  Outgoing update filter list for all interfaces is not set ②
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 23 seconds ③
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip                                    ④
  Default version control: send version 1, receive any version ⑤
    Interface          Send Recv Triggered RIP Key-chain
  FastEthernet0/0      1     1 2
  Serial1/1            1     1 2
  Loopback0            1     1 2
  Automatic network summarization is in effect            ⑥
  Maximum path: 4                                         ⑦
  Routing for Networks:                                   ⑧
    1.0.0.0
    12.0.0.0
    13.0.0.0
  Routing Information Sources:                             ⑨
    Gateway         Distance      Last Update
  13.1.1.3          120          00:00:03
  12.1.1.2          120          00:00:07
  Distance: (default is 120)                             ⑩

```

① 显示运行了 RIP 协议。

② 外出和进入方向都没有使用过滤列表，这是 CCIE 考试的内容。

③ RIP 定时器的设置值。

④ 重分布中只有 RIP，意味着这里只接收和发送 RIP 路由协议，在 CCNP 中会学到重分布其他路由协议，即多个路由协议共同工作。

⑤ 当前运行的是 RIPv1，发送版本 1 的信息，接收版本 1 和版本 2 的信息，本书在 RIPv2 部分再详细讨论这个问题。

⑥ 路由自动汇总是起作用的。

⑦ 负载均衡路径数据的设置，默认是 4，最大可以是 6。

⑧ 路由器直连的有类网络信息。

⑨ RIP 从哪些路由器收到更新信息、路由的下一跳地址、管理距离、收到最后一次更新的时间。

⑩ 管理距离是 120。

6. debug ip rip 命令

在路由器 R1 上使用“debug ip rip”命令查看路由器的输出信息，部分输出显示如下：

```

R1#debug ip rip
RIP protocol debugging is on
R1#
*Mar 1 05:09:06.666: RIP: received v1 update from 13.1.1.3 on FastEthernet0/0
*Mar 1 05:09:06.670:      2.0.0.0 in 2 hops
*Mar 1 05:09:06.674:      3.0.0.0 in 1 hops
*Mar 1 05:09:06.674:      23.0.0.0 in 1 hops
*Mar 1 05:09:11.262: RIP: sending v1 update to 255.255.255.255 via Serial1/1 (12.1.1.1)
*Mar 1 05:09:11.266: RIP: build update entries
*Mar 1 05:09:11.266:   network 1.0.0.0 metric 1
*Mar 1 05:09:11.270:   network 3.0.0.0 metric 2
*Mar 1 05:09:11.270:   network 13.0.0.0 metric 1
*Mar 1 05:09:14.418: RIP: sending v1 update to 255.255.255.255 via Loopback0 (1.1.1.1)
*Mar 1 05:09:14.422: RIP: build update entries
*Mar 1 05:09:14.422:   network 2.0.0.0 metric 2
*Mar 1 05:09:14.426:   network 3.0.0.0 metric 2
*Mar 1 05:09:14.426:   network 12.0.0.0 metric 1

```

```
*Mar 1 05:09:14.430: network 13.0.0.0 metric 1
*Mar 1 05:09:14.430: network 23.0.0.0 metric 2
```

上面是部分 Debug 的输出信息,从这些输出信息中可以得出下面的结论:“received v1”和“sending v1”说明运行的是 RIP 的版本 1;从“sending v1 update to 255.255.255.255”得知 RIPv1 是广播式更新;从 R3 发过来的更新信息:

```
*Mar 1 05:09:06.666: RIP: received v1 update from 13.1.1.3 on FastEthernet0/0
*Mar 1 05:09:06.670: 2.0.0.0 in 2 hops
*Mar 1 05:09:06.674: 3.0.0.0 in 1 hops
*Mar 1 05:09:06.674: 23.0.0.0 in 1 hops
```

可以发现没有包含网络 1.0.0.0、12.0.0.0,这说明在路由器 R3 的 Fa0/0 接口启用了水平分割, R3 从 R1 学到的路由不再向 R1 发送。启用水平分割的接口也不会发送直连接口的路由,所以 R3 也不向 R1 通告 13.0.0.0。类似地,可以得出路由器 R1、R2、R3 的所有接口,在默认情况下都启用了水平分割,可以使用“show ip interface”命令查看所有接口水平分割的启用情况,接下来会介绍如何禁用水平分割;从“sending v1 update to 255.255.255.255 via Loopback0 (1.1.1.1)”得知路由器 R1 也会向 Loopback 0 发送更新消息,环回接口是一个虚拟的路由接口,发送更新消息除了浪费资源外,没有什么实质性的意义,稍后会介绍如何关闭这样的消息。

7. 水平分割

从上面 Debug 的输出信息中,可以看出水平分割的开启情况,在路由器 R1 上使用“show ip interface fa 0/0”命令,查看 Fa0/0 接口水平分割的情况,部分显示如下:

```
R1#show ip int fa 0/0
省略部分输出。
Split horizon is enabled
省略部分输出。
```

从上面的输出中进一步验证 R1 的 Fa0/0 接口的水平分割是开启的,在路由器 R1 上使用下面的命令禁用 Fa0/0 接口的水平分割:

```
R1(config)#int fa 0/0
R1(config-if)#no ip split-horizon
```

再次查看 R1 上“debug ip rip”命令的输出,显示如下:

```
*Mar 1 05:34:25.450: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0
(13.1.1.1)
*Mar 1 05:34:25.454: RIP: build update entries
*Mar 1 05:34:25.454: network 1.0.0.0 metric 1
*Mar 1 05:34:25.458: network 2.0.0.0 metric 2
*Mar 1 05:34:25.458: network 3.0.0.0 metric 2
*Mar 1 05:34:25.462: network 12.0.0.0 metric 1
*Mar 1 05:34:25.462: subnet 13.1.1.0 metric 1
*Mar 1 05:34:25.466: network 23.0.0.0 metric 2
```

从上面的输出中可以看出,禁用水平分割后, R1 向 R3 发送的更新包中包括了整个路由表的所有条目。使用“show ip int fa 0/0”命令可以看到“Split horizon is disabled”的输出。

8. 被动接口的配置 (Passive-interface)

从前面 Debug 的输出中,可以看到 RIP 进程也向环回接口发送路由更新包,这样做除了浪费资源外没有任何意义,对于这样的接口,可以使用下面的命令关闭某个接口更新包的发送:

```
R1(config)#router rip
R1(config-router)#passive-interface loopback 0
```

把 Loopback 0 设成被动接口后, 该接口不再往外发送路由更新包, 但仍然会接收其他路由器发过来的路由更新包。

9. 单播更新

在图 6-2-1 中, 通过配置单播更新, 实现路由器 R1 和 R2 之间可以相互学习路由, 但都不与 R3 交互路由。读者可以配置 CCNA 模拟机架中的 R1、R2、R3 来验证单播更新的配置。R1 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#no cdp run
R1(config)#int fa 0/0
R1(config-if)#ip add 123.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config-if)#router rip
R1(config-router)#net 1.0.0.0
R1(config-router)#net 123.0.0.0
R1(config-router)#passive-interface default
```

该命令把所有运行 RIP 协议的端口设成被动端口, Loopback 和 fa 0/0 都被设成了被动接口, 都不向外发送路由更新包。如果某个接口需要发送路由更新包, 则可以使用 no passive-interface 接口名和编号, 来允许某个接口发送路由更新包。

```
R1(config-router)#neighbor 123.1.1.2
```

neighbor 命令, 指定 123.1.1.2 为邻居, R1 上的路由更新包将以单播的形式发送给 123.1.1.2 路由器。

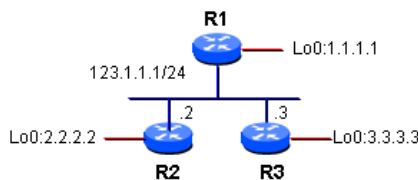


图 6-2-1 单播更新

R2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#no cdp run
R2(config)#int fa 0/0
R2(config-if)#ip add 123.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int lo0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
R2(config-if)#router rip
R2(config-router)#net 2.0.0.0
R2(config-router)#net 123.0.0.0
R2(config-router)#passive-interface default
R2(config-router)#neighbor 123.1.1.1
```

R3 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#no cdp run
R3(config)#int fa 0/0
R3(config-if)#ip add 123.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo0
```



```
R3(config-if)#ip add 3.3.3.3 255.255.255.0
R3(config-if)#router rip
R3(config-router)#net 3.0.0.0
R3(config-router)#net 123.0.0.0
R3(config-router)#passive-interface default
```

分别使用“show ip route”命令查看路由器 R1、R2 和 R3 的路由表，可以发现 R1 和 R2 彼此可以学到对方的路由，R3 学不到 R1 和 R2 上的路由。在路由器 R1 上执行“debug ip rip”命令，可以看到下面所示的单播更新包：

```
*Mar 1 00:19:48.323: RIP: sending v1 update to 123.1.1.2 via FastEthernet0/0 (123.1.1.1)
*Mar 1 00:19:48.327: RIP: build update entries
*Mar 1 00:19:48.327: network 1.0.0.0 metric 1
*Mar 1 00:20:01.511: RIP: received v1 update from 123.1.1.2 on FastEthernet0/0
*Mar 1 00:20:01.515: 2.0.0.0 in 1 hops
```

10. 触发更新

距离矢量路由协议采用的是周期性更新，可以在串行接口上使用触发更新，以太网接口不支持触发更新。配置串行接口触发更新的命令如下：

```
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0 接口一定要配置 IP 地址，启用 IP 协议。
R1(config-if)#ip rip triggered 启用触发更新。
```

可以使用“no ip rip triggered”命令关闭触发更新。

11. 默认路由

在图 6-2-2 中，某企业内部运行 RIP 协议，R1 是企业内部路由器，R2 是企业边界路由器，R3 相当于 ISP 的边界路由器。R2 使用 RIP 协议与内部相连，配置默认路由与 Internet 相连；R3 配置静态路由访问企业内部网络；R1 是企业内部路由器，可以通过 RIP 学到整个企业内部的路由，可如何访问 Internet 呢？如果是在内部每台路由器上都配置默认路由，不但麻烦且不能适应网络拓扑的变化，此时就需要在路由器 R2 上使用“ip default-network”或“default-information originate”命令向内部网络宣告一条动态的默认路由。

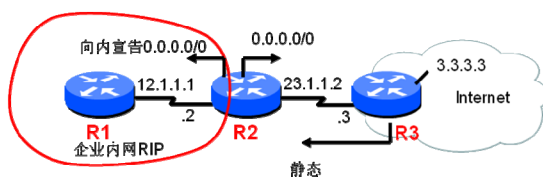


图 6-2-2 宣告默认路由

该实验的 IP 地址分配如图 6-2-2 中所示，路由器 R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#router rip
R1(config-router)#net 12.0.0.0
```

路由器 R2 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
```

```

R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
{
R2(config-if)#router rip
R2(config-router)#net 12.0.0.0
R2(config-router)#net 23.0.0.0
R2(config-router)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 23.1.1.3
配置默认路由, 对所有未知的网络都发往 ISP 的接入路由器。
R2(config)#ip default-network 23.0.0.0
配置默认网络, ip default-network 仅支持有类网络后面要写网络的主类地址。
}

```

也可以用下面一段的配置替换括号中的一段配置:

```

R2(config-if)#router rip
R2(config-router)#net 12.0.0.0
R2(config-router)# default-information originate
声明路由器 R2 是默认路由的起源, 这样 R2 就会向其他的 RIP 路由器, 宣告自己是默认路由。
R2(config-router)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 23.1.1.3 配置默认路由, 对所有未知的网络
都发往 ISP 的接入路由器。

```

路由器 R3 的配置如下:

```

Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
R3(config-if)#exit
R3(config)#ip route 12.1.1.0 255.255.255.0 23.1.1.2

```

在路由器 R1 上使用“show ip route”命令查看路由表, 显示如下:

```

R1#show ip route

12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/1
R*   0.0.0.0/0 [120/1] via 12.1.1.2, 00:00:10, Serial1/1

```

从上面的输出中, 可以看到 R1 学到一条“R* 0.0.0.0/0 [120/1]”的路由, 这是一条默认路由, 但不是静态的默认路由, 而是通过 RIP 学到的一条默认路由。

12. 浮动静态路由

在图 6-2-3 中, 某公司的总部和分部间使用专线相连, 配置 RIP 协议实现公司网络的互连。为了防止专线故障, 又申请了一根拨号的备份线路提供冗余, 以备在专线链路故障时, 使用拨号线路。因为拨号线路带宽有限, 使用动态路由协议, 路由更新包会占用部分带宽, 为了不影响关键的业务流, 在拨号线路上配置静态路由。

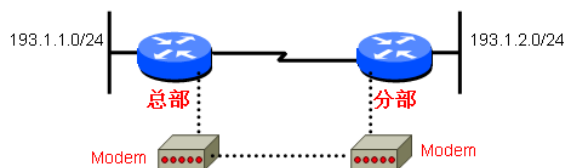


图 6-2-3 浮动静态路由示意

把上面的网络示意图使用如图 6-2-4 所示的网络拓扑替代, 把 R1 和 R2 之间的快速以太网线路想象成图 6-2-3 中的快速专用线路, 把 R1 和 R2 之间的慢速串行线路想象成图 6-2-3 中的慢速拨号线路。在以太网上运行 RIP 协议, 以太网正常时, 193.1.1.0/24 和 193.1.2.0/24 之间的流量从以太网走, 当以太网出现故障时, 193.1.1.0/24 和 193.1.2.0/24 之间的流量从串行线路走。

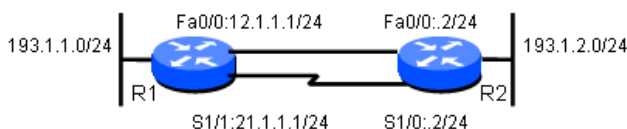


图 6-2-4 浮动静态路由拓扑

路由器 R1 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#no cdp run
R1(config)#int fa 0/0
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int s1/1
R1(config-if)#ip add 21.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ip add 193.1.1.1 255.255.255.0
R1(config-if)#router rip
R1(config-router)#net 12.0.0.0
```

宣告快速线路, 快速线路是运行 RIP 协议的。不要宣告 21.0.0.0, 因为这里的串行线路相当于拨号的慢速线路, 为了节省带宽, 是不运行动态路由协议的。

R1(config-router)#net 193.1.1.0 宣告总部的内部网络。

R1(config-router)#exit

R1(config)#ip route 193.1.2.0 255.255.255.0 21.1.1.2 130

创建去往分部内部网络的静态路由, 这里配置的是从慢速的串行线路走, 130 是管理距离, 这个值的配置是有讲究的, 一定要大于 RIP 的管理距离 120。假设这里没有使用管理距离, 静态路由由默认的管理距离是 1, 同样的, 193.1.2.0/24 这条路由, 通过 RIP 和静态路由都学到了, 比较两种路由的管理距离, 结果静态路由的管理距离小, 静态路由进入了路由表, 总部去分部的所有流量都从慢速线路走, 快速的线路闲置不用。如果把静态路由的管理距离设成 130, 静态路由和 RIP 路由进行比较, RIP 路由的管理距离小, RIP 路由进入了路由表, 总部去分部的流量都从快速的以太网走, 当以太网线路出现故障时, RIP 路由消失, 此时管理距离是 130 的静态路由就起作用了。

路由器 R2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#no cdp run
R2(config)#int fa 0/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/0
R2(config-if)#ip add 21.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int lo0
R2(config-if)#ip add 193.1.2.1 255.255.255.0
R2(config-if)#router rip
R2(config-router)#net 12.0.0.0 解释类似上面的 R1。
R2(config-router)#net 193.1.2.0 解释类似上面的 R1。
R2(config-router)#exit
R2(config)#ip route 193.1.1.0 255.255.255.0 21.1.1.1 130 解释类似上面的 R1。
```

配置完成后，使用“show ip route”命令查看路由器 R1 的路由表，显示如下：

```
R1#show ip route
      21.0.0.0/24 is subnetted, 1 subnets
C       21.1.1.0 is directly connected, Serial1/1
C       193.1.1.0/24 is directly connected, Loopback0
      12.0.0.0/24 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, FastEthernet0/0
R       193.1.2.0/24 [120/1] via 12.1.1.2, 00:00:18, FastEthernet0/0
```

从上面的输出中，可以看到总部（R1）去往分部网络（R2 上的 193.1.2.0/24）的路由是从快速线路（100Mb/s 的以太网）走。关闭路由器 R1 和路由器 R2 的 Fa0/0 接口，之所以要关闭两端的接口，是因为 R1 和 R2 不是直连，中间还有一台交换机，关闭一端的接口，另一端的接口不会 Down 掉。关闭路由器 R1 和路由器 R2 的 Fa0/0 接口后，在路由器 R1 上使用“show ip route”命令，显示如下：

```
R1#show ip route
      21.0.0.0/24 is subnetted, 1 subnets
C       21.1.1.0 is directly connected, Serial1/1
C       193.1.1.0/24 is directly connected, Loopback0
S       193.1.2.0/24 [130/0] via 21.1.1.2
```

从上面的输出中，可以看到 RIP 路由消失，静态路由出现，静态路由的管理距离是 130。当快速线路故障后，慢速线路开始启用。

13. 更改定时器的值

可以使用命令更改 RIP 定时器，命令格式如下：

```
Router(config)#router rip
Router(config-router)#timers basic [Interval between updates] [Invalid] [Holddown]
[Flush]
```

比如把 RIP 的路由更新定时器改成 40 秒，路由失效定时器改成 240 秒，路由抑制定时器改成 0 秒，路由刷新定时器改成 320 秒，可以使用下面的命令来实现：

```
Router(config-router)#timers basic 40 240 0 320
```

使用“show ip protocols”命令进行验证，部分显示如下：

```
Router#show ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 40 seconds, next due in 0 seconds
  Invalid after 240 seconds, hold down 0, flushed after 320
```

从上面的输出中，可以发现 RIP 定时器更改已经生效。除非很熟悉，一般不建议修改默认定时器的值。



6.3 VLSM 和 CIDR***

随着 Internet 的飞速发展，可用的 IP 地址越来越少，路由表却越来越大，核心 Internet 路由器处理能力也逐渐耗尽。为了克服这些问题，VLSM（Variable Length Subnet Masking，变长子网掩码）技术被用来节约 IP 地址的使用，CIDR（Classless Inter-Domain Routing，无类域间路由）技术被用来减小路由表的大小。

6.3.1 VLSM***

1. 使用 VLSM

传统的 A、B、C 类使用固定长度的子网掩码。在第 2 章中，介绍了子网的划分，通过使用比传统 8 位、16 位、24 位更小的子网掩码长度来实现子网的划分。第 2 章中介绍的是固定长度子网掩码的划分，本节介绍一种可变长度子网掩码的技术，即对部分子网再次进行子网划分。

VLSM 允许一个组织在同一个网络地址空间中使用多个子网掩码。利用 VLSM，管理员可以对子网再进行子网划分，使寻址效率更高。接下来讨论一下固定子网掩码长度的限制，本书第 2 章 2.5.5 节中的例 1 提到某单位申请到了一个 C 类的网络地址 199.1.1.0/24，该单位共有 5 个部门，每个部门最多只会有 28 台计算机。为了增强安全性，使用路由器来限制部门之间只能进行有限的访问。问子网掩码设成多少比较合适？每个部门使用的 IP 地址范围是多少？第 2 章给出的解法是使用 27 位的子网掩码，把一个 C 类地址分成 8 个子网（忽略全“0”和全“1”的子网，还有 6 个可用的子网，不过在较新的思科 IOS 版本中，可以使用“Router(config)#ip subnet-zero”来支持全“0”和全“1”子网），每个子网中可以容纳 30 台计算机。试想一下，如果 5 个部门的计算机数量分布如图 6-3-1 所示，该如何划分子网掩码呢？

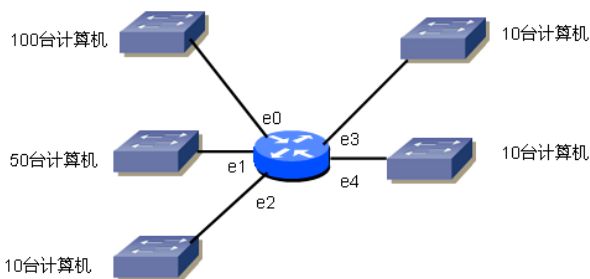


图 6-3-1 VLSM 需求

从图 6-3-1 中可以看出，有一个部门有 100 台计算机，还有一个部门有 50 台计算机，其他三个部门各有 10 台计算机，如果使用第 2 章介绍的固定长度子网掩码的做法，将无法满足 IP 地址的需求。这里介绍使用 VLSM 的计算方法，如图 6-3-2 所示。

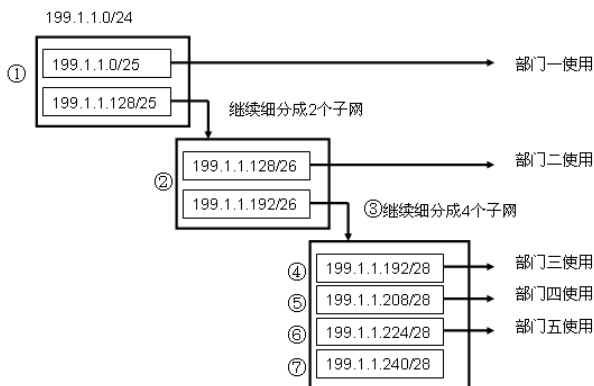


图 6-3-2 VLSM 计算

① 为了满足一个子网中可以容纳 100 台计算机, 该子网主机位的位数至少要满足 7 位 ($2^7-2=126$), 可以从主机位的 8 位中借出 1 位作为子网位, 可以划分成 2 个子网, 0 和 1 子网, 即 199.1.1.0/25 和 199.1.1.128/25。需要使用 ip subnet-zero 来支持全“0”和全“1”的子网, 给第一个部门分配 199.1.1.0/25 子网, IP 地址范围从 199.1.1.0~127, 199.1.1.0 是该子网的网络号, 199.1.1.1 是该子网中第一个可用 IP 地址, 假使分配给路由器的 e0 接口, 199.1.1.127 是该子网的广播地址, 该子网中计算机可用的 IP 地址范围是 199.1.1.2~126。

② 199.1.1.0/24 被分成两个子网后, 199.1.1.0/25 子网已经被分配出去, 还剩下一个子网 199.1.1.128/25。这个子网需要满足余下 4 个部门的需求, 考虑到有一个部门的计算机数量是 50, 需要占用 199.1.1.128/25 子网 7 位主机位中 6 位 ($2^6-2=62$), 多出的 1 位继续划分成 2 个子网, 即 199.1.1.128/26 和 199.1.1.192/26。把 199.1.1.128/26 子网分配给部门二使用, IP 地址范围从 199.1.1.128~191, 199.1.1.128 是该子网的网络号, 199.1.1.129 是该子网中第一个可用 IP 地址, 假使分配给路由器的 e1 接口, 199.1.1.191 是该子网的广播地址, 该子网中计算机可用的 IP 地址范围是 199.1.1.130~190。

③ 199.1.1.128/25 被分成两个子网后, 199.1.1.128/26 子网已经被分配出去, 还剩下一个子网 199.1.1.192/26。这个子网需要满足余下 3 个部门的需求, 考虑到每个部门的计算机数量是 10, 需要占用 199.1.1.192/26 子网 6 位主机位中 4 位 ($2^4-2=14$), 多出的 2 位可以划分成 4 个子网, 即 199.1.1.192/28、199.1.1.208/28、199.1.1.224/28、199.1.1.240/28。

④ 把 199.1.1.192/28 子网分配给部门三使用, IP 地址范围从 199.1.1.192~207, 199.1.1.192 是该子网的网络号, 199.1.1.193 是该子网中第一个可用 IP 地址, 假使分配给路由器的 e2 接口, 199.1.1.207 是该子网的广播地址, 该子网中计算机可用的 IP 地址范围是 199.1.1.194~206。

⑤ 把 199.1.1.208/28 子网分配给部门四使用, IP 地址范围从 199.1.1.208~223, 199.1.1.208 是该子网的网络号, 199.1.1.209 是该子网中第一个可用 IP 地址, 假使分配给路由器的 e3 接口, 199.1.1.223 是该子网的广播地址, 该子网中计算机可用的 IP 地址范围是 199.1.1.210~222。

⑥ 把 199.1.1.224/28 子网分配给部门五使用, IP 地址范围从 199.1.1.224~239, 199.1.1.224 是该子网的网络号, 199.1.1.225 是该子网中第一个可用 IP 地址, 假使分配给路由器的 e4 接口, 199.1.1.239 是该子网的广播地址, 该子网中计算机可用的 IP 地址范围是 199.1.1.226~238。

⑦ 199.1.1.240/28 子网是多出来的一个子网, 可以留给以后新的部门使用。

经过计算, 每个部门计算机和路由接口的 IP 地址分配如图 6-3-3 所示。从图中可以看到, 部门一所在的子网是 199.1.1.0/25, 部门二所在的子网是 199.1.1.128/26, 部门三所在的子网是 199.1.1.192/28, 部门四所在的子网是 199.1.1.208/28, 部门五所在的子网是 199.1.1.224/28。5 个部门使用了 3 种子网掩码长度, 这就是 VLSM 的应用, VLSM 使 IP 地址的分配更加灵活, 应用更加高效。

在如图 6-3-4 所示的广域网链路上, 为了更高效地利用 IP 地址, 网络位的长度可以是 30, 使用 255.255.255.252 的子网掩码, 每个网络中可以使用的 IP 地址的个数是 $2(2^2-2=2)$, 刚好可以配在广域网的点对点链路两端。

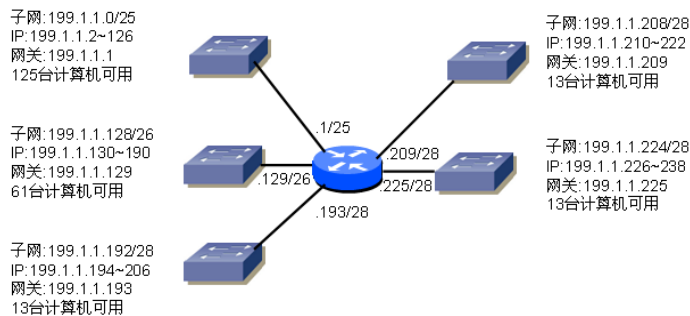


图 6-3-3 VLSM IP 地址分布

ip unnumbered

在如图 6-3-4 所示的广域网链路中，两台路由器的串口上必须配有 IP 地址，才能实现互通。可保留给路由器串口的 IP 地址实际上仅仅用于实现路由器间的互通，除此之外再没有别的用途了。在这样一种背景下，借用 IP 地址（ip unnumbered）的应用就产生了。

在图 6-3-5 中，路由器 R1 和 R2 通过串行接口相连，为了节省 IP 地址的使用，串行接口可以借用路由器其他接口的 IP 地址，但两台路由器的串行接口不在同一个网段，需要配置到对端去的静态路由。

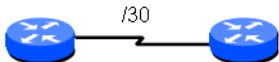


图 6-3-4 广域网链路



图 6-3-5 ip unnumbered 应用

路由器 R1 的配置如下:

```
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int s1/1
R1(config-if)#ip unnumbered fa 0/0      S1/1 借用 Fa0/0 接口的 IP 地址。
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#ip route 192.168.2.0 255.255.255.0 s1/1
```

路由器 R1 的 S1/1 和路由器 R2 的 S1/0 接口的 IP 地址并不在一个网段内，需要配置静态路由，使路由器 R1 可以到达路由器 R2 192.168.2.0/24 网段的路由。

路由器 R2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int fa 0/0
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/0
R2(config-if)#ip unnumbered fa 0/0      S1/0 借用 Fa0/0 接口的 IP 地址。
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip route 192.168.1.0 255.255.255.0 s1/0
```


路由器 R2 的 S1/0 和路由器 R1 的 S1/1 接口的 IP 地址并不在一个网段内，需要配置静态路由，使路由器 R2 可以到达路由器 R1 192.168.1.0/24 网段的路由。

在路由器 R1 上 ping 192.168.2.1 进行测试，显示如下：

```
R1#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/20/44 ms
R1#
```

至此，路由器 R1 和 R2 的串行接口没有占用 IP 地址，也实现了两边以太网的互连。

2. 使用 VLSM 的注意事项

使用 VLSM 虽然可以节省 IP 地址，但要根据使用的是什么样的网络协议，RIPv1 和 IGRP 是有类路由协议，无法支持 VLSM。静态路由、RIPv2、EIGRP、OSPF、IS-IS 和 BGP 都是无类路由协议，都支持 VLSM。下一节将结合配置演示 RIPv1 不支持 VLSM，RIPv2 可以支持 VLSM。

6.3.2 CIDR**

1. 使用 CIDR

在一个有类别的系统中，路由器决定一个地址的类别，并根据该类别识别网络和主机。而在 CIDR 中，路由器使用前缀来描述有多少个位是网络位（或称前缀），剩下的位则是主机位。表示前缀的数字跟在地址的结尾，用斜杠（“/”）来表示，例如 192.168.1.0/30，这里的“/30”是前缀。一个地址的网络和主机部分不再受完整 8 位组的限制，比如 A 类地址的网络位是 8 位，B 类地址的网络位是 16 位，C 类地址的网络位是 24 位。

CIDR 显著提高了 IPv4 的可扩展性和效率，通过使用路由聚合（也称超网），可有效地减小路由表的大小，节省路由器的内存空间，提高路由器的查找效率。第 2 章 2.5.5 节的例 3 就是 CIDR 的一个具体应用。这里再举一个例子，南京工业大学接入了中国教育科研网，因为上网的用户数众多，申请了 16 个 C 类的 IP 地址，从 202.119.240.0~202.119.255.255，假如没有使用 CIDR，教育网的骨干路由器需要有 16 条静态路由指向南京工业大学，使用 CIDR 后，用第 2 章 2.5.5 节的汇总方法对连续的 16 个 C 类地址进行汇总后，教育网的骨干路由器只要配置 202.119.240.0/20 的路由指向南京工业大学就可以了，大大减小了路由表的大小。

2. 使用 CIDR 的注意事项

使用 CIDR 虽然有很多优势，但和使用 VLSM 一样，也要根据使用的是什么样的网络协议，RIPv1 和 IGRP 是有类路由协议，无法支持 CIDR。静态路由、RIPv2、EIGRP、OSPF、IS-IS 和 BGP 都是无类路由协议，都支持 CIDR。下一节将结合配置演示 RIPv1 不支持 CIDR，RIPv2 可以支持 CIDR。



6.4 RIPv2***

本节主要讨论 RIPv1 的局限性，以及 RIPv2 具有的增强特性。

6.4.1 RIPv1 的局限性***

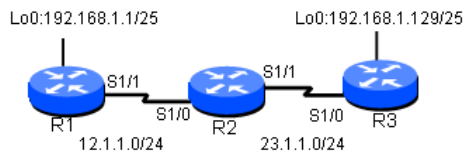


图 6-4-1 不连续子网的网络

通过前面的介绍，大家已经了解到 RIPv1 是一个距离矢量路由选择协议，使用跳计数作为唯一的度量值，15 是最大跳数，在默认情况下，每 30 秒发送一次广播更新。此外，还了解到 RIPv1 是一个有类路由协议，不支持 VLSM 和 CIDR。

1. RIPv1 不支持不连续的子网

使用 RIPv1 完成如图 6-4-1 所示的配置。

路由器 R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ip add 192.168.1.1 255.255.255.128
注意这里配置的 IP 地址和子网掩码，网络位是 25 位，即把 192.168.1.0/24 分成了两个子网，这里使用 192.168.1.0/25 子网，因为这里使用了全“0”的子网，在老版的思科 IOS 中一定要使用 ip subnet-zero 来支持全“0”和全“1”的子网。CCNA 模拟机架的路由器 R1、R2、R3 配置的 IOS 默认使用的就是 ip subnet-zero，所以这里并没有配置该语句。如果读者使用 no ip subnet-zero 取消对全“0”和全“1”子网的支持，然后再配置这样的 IP 地址，就会出现“Badmask /25 for address 192.168.1.1”的出错提示。
R1(config-if)#router rip
R1(config-router)#net 12.0.0.0
R1(config-router)#net 192.168.1.0 这里使用的仍然是主类网络地址。
```

路由器 R2 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#router rip
R2(config-router)#net 12.0.0.0
R2(config-router)#net 23.0.0.0
```

路由器 R3 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo0
R3(config-if)#ip add 192.168.1.129 255.255.255.128
R3(config-if)#router rip
R3(config-router)#net 23.0.0.0
R3(config-router)#net 192.168.1.0
```

在路由器 R2 上，测试网络的连通性，测试结果如下：

```
R2#ping 192.168.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/11/16 ms
R2#ping 192.168.1.129

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.129, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R2#
```

从上面的输出中，可以看出 R2 去往 192.168.1.1 是通的，去往 192.168.1.129 是不通的，会不会是因为 R2 上的路由配置不正确呢？在路由器 R2 上使用“show ip route”命令，查询 R2 的路由表，显示如下：

```
R2#show ip route

      23.0.0.0/24 is subnetted, 1 subnets
C       23.1.1.0 is directly connected, Serial1/1
      12.0.0.0/24 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, Serial1/0
R       192.168.1.0/24 [120/1] via 23.1.1.3, 00:00:08, Serial1/1
              [120/1] via 12.1.1.1, 00:00:24, Serial1/0
```

从上面的输出中，可以看到路由器 R2 去往 192.168.1.0/24 的路由有两个下一跳，即去往 R1 或 R3 都可，默认将使用负载均衡，即去往 192.168.1.1 和去往 192.168.1.129 的数据包都应该一个往左一个往右，可结果为何却是去往 192.168.1.1 都通了，去往 192.168.1.129 却一个也没通。出现这种现象的原因是，思科路由器默认使用的是快速交换，第一个数据包查询路由表，后续的数据包都根据第一个数据的缓存路径进行转发，刚好 192.168.1.1 的第一个 ping 包往左，后续的所有去往 192.168.1.0/24 的数据包都往左，这就出现了前面现象。关闭路由器 R2 的快速交换，启用进程交换（每个数据包都查询路由表，这样路由器的处理速度会变慢）。

```
R2#conf t
R2(config)#no ip cef
```

再次在路由器 R2 上 ping 192.168.1.1 和 192.168.1.129，结果显示如下：

```
R2#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
U!..!U
Success rate is 40 percent (2/5), round-trip min/avg/max = 4/8/12 ms
R2#ping 192.168.1.129

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.129, timeout is 2 seconds:
U!..!U
Success rate is 40 percent (2/5), round-trip min/avg/max = 4/6/8 ms
```

从上面的输出中可以看到 R2 发往 192.168.1.1 和 192.168.1.129 的数据包都是一个通一个不通，路由器 R2 根据路由表负载均衡，结果造成 ping 包的发送方向一个正确一个不正确。出现这种现象的原因是因为 RIPv1 是一个有类路由协议，会在主类网络的边界自动汇总，并且这种汇总是关闭不了的。在路由器 R1 上执行“debug ip rip”命令，查看路由器 R1 发往 R2 的 RIP 更新，显示如下：

```
R1#debug ip rip
RIP protocol debugging is on
```

```

R1#
*Mar 1 00:02:39.447: RIP: sending v1 update to 255.255.255.255 via Serial1/1 (12.1.1.1)
*Mar 1 00:02:39.451: RIP: build update entries
*Mar 1 00:02:39.451: network 192.168.1.0 metric 1

```

从上面的输出中，可以看出路由器接口启用了水平分割，还可以看出 R1 向 R2 发送的路由表中包含了 192.168.1.0，这个输出可能说明不了问题，因为 R1 Loopback 0 口所在的网络号也是 192.168.1.0。在路由器 R3 上执行“debug ip rip”命令，查看路由器 R3 发往 R2 的 RIP 更新，显示如下：

```

R3#debug ip rip
RIP protocol debugging is on
R3#
*Mar 1 00:06:23.595: RIP: received v1 update from 23.1.1.2 on Serial1/0
*Mar 1 00:06:23.599: 12.0.0.0 in 1 hops
*Mar 1 00:06:27.843: RIP: sending v1 update to 255.255.255.255 via Serial1/0 (23.1.1.3)
*Mar 1 00:06:27.847: RIP: build update entries
*Mar 1 00:06:27.847: network 192.168.1.0 metric 1

```

从上面的输出中，可以看到路由器 R2 把自己的直连网络 12.1.1.0/24 汇总成主类网络 12.0.0.0 向 R3 发送，读者可能会问，路由器 R2 怎么没有把从 R1 上学过来的 192.168.1.0 向 R3 发送呢？这是因为 R3 也把自己的网络汇总成 192.168.1.0 向 R2 发送了，因为水平分割的原因，R2 不会把同样的路由再发回来，即使关闭水平分割，R2 把 192.168.1.0 发给 R3，因为 RIPv1 是一个有类路由协议，既然 R3 已经有同样主类网络的直连路由，它不会学习 RIP 通告过来的这个主类网络。从 R3 向 R2 发送的更新中，可以看出 R3 并没有发送环回接口的网络号 192.168.1.128，而是发送了环回接口所在主类网络的网络地址。

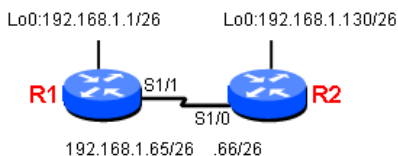


图 6-4-2 连续的子网掩码长度相同的网络

例子，路由器 R1 的配置如下：

```

Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 192.168.1.65 255.255.255.192
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ip add 192.168.1.1 255.255.255.192
R1(config-if)#router rip
R1(config-router)#net 192.168.1.0

```

因为 R1 的 Lo0 和 S1/1 接口都包含在主类网络 192.168.1.0 中，这里只要写一次主类网络号就可以了。

路由器 R2 的配置如下：

```

Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 192.168.1.66 255.255.255.192
R2(config-if)#no shut
R2(config-if)#int lo0
R2(config-if)#ip add 192.168.1.130 255.255.255.192

```

```
R2(config-if)#router rip
R2(config-router)#net 192.168.1.0
```

在路由器 R1 上执行 “debug ip rip” 命令，显示如下：

```
R1#
*Mar 1 00:42:40.451: RIP: sending v1 update to 255.255.255.255 via Serial1/1
(192.168.1.65)
*Mar 1 00:42:40.455: RIP: build update entries
*Mar 1 00:42:40.455: subnet 192.168.1.0 metric 1
*Mar 1 00:42:45.559: RIP: received v1 update from 192.168.1.66 on Serial1/1
*Mar 1 00:42:45.563: 192.168.1.128 in 1 hops
```

从上面的输出中，可以发现 R1 向 R2 发送了 192.168.1.0 的路由，可到底是 192.168.1.0/24 这个主类网络号呢，还是 192.168.1.0/26 这个子网网络号呢？这里是不太清楚的，因为 RIPv1 发送路由更新的时候不携带子网掩码。但从 R2 发送过来的路由更新 192.168.1.128，可以判定 RIPv1 在非主类网络的边界是不会自动产生汇总的。

在路由器 R2 上执行 “debug ip rip” 命令，显示如下：

```
*Jun 24 00:39:38.391: RIP: received v1 update from 192.168.1.65 on Serial1/0
*Jun 24 00:39:38.391: 192.168.1.0 in 1 hops
*Jun 24 00:39:41.447: RIP: sending v1 update to 255.255.255.255 via Serial1/0
(192.168.1.66)
*Jun 24 00:39:41.451: RIP: build update entries
*Jun 24 00:39:41.451: subnet 192.168.1.128 metric 1
```

从上面的输出中，可以看到 R2 发出的路由是 192.168.1.128，进一步验证在非主类网络的边界，RIPv1 不会自动汇总。R2 从 R1 收到了 192.168.1.0，R2 如何看待这条路由，是当成 “/24” 还是 “/26” 的路由条目呢？在 R2 上执行 “show ip route” 命令，显示如下：

```
R2#show ip route
192.168.1.0/26 is subnetted, 3 subnets
C 192.168.1.64 is directly connected, Serial1/0
R 192.168.1.0 [120/1] via 192.168.1.65, 00:00:18, Serial1/0
C 192.168.1.128 is directly connected, Loopback0
```

读者是不是很惊讶，R2 很聪明，居然知道 R1 发送过来的是 “/26”。其实不是这样的，RIPv1 是一个有类路由协议，当从一个接口收到同一个主类网络的子网路由时，路由器认为收到的子网路由与接收接口的网络位相同。R2 从 R1 收到 192.168.1.0，并没有携带子网掩码，R2 认为这条路由的掩码位数与接收接口 S1/0 的子网掩码位数相同，即 “/26”。如果发送过来的路由的网络位数与接收接口的网络位数不同（也就是在 VLSM 的情况下），会出现什么情况呢？接下来介绍 RIPv1 不支持 VLSM。

2. RIPv1 不支持 VLSM

在图 6-4-2 中，RIPv1 可以正常工作，在图 6-4-3 中，使用了 VLSM，RIPv1 运行的结果如何呢？

注意：图中两个串行接口的子网掩码长度是 “/30”，在这样的网络中仅容纳 2 个 IP 地址，刚好可以满足广域网的互连。在前面实验的基础上，只要把两台路由器串行接口的子网掩码改成 255.255.255.252 就可以了，这里不再列出配置。在路由器 R1 上马上执行 “show ip route” 命令，查看路由器 R1 的路由表，显示如下：

```
R1#show ip route
```

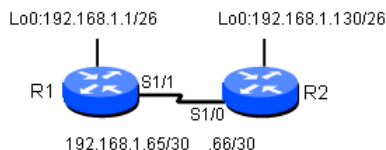


图 6-4-3 VLSM 的网络

```

192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C    192.168.1.64/30 is directly connected, Serial1/1
C    192.168.1.0/26 is directly connected, Loopback0
R    192.168.1.128/30 [120/1] via 192.168.1.66, 00:00:17, Serial1/1
R    192.168.1.128/26 [120/1] via 192.168.1.66, 00:00:28, Serial1/1

```

从上面的输出中, 可以看到 R1 的路由表中有 192.168.1.128/26 和 192.168.1.128/30 两条路由。存在第一条 (“/26”), 是因为第一条是以前学到的, RIP 删除一条路由默认的定时器是 240 秒。存在第二条 (“/30”), 是因为先更改了路由器 R1 的 S1/1 接口的 IP 子网掩码为 30 位, 此时路由器 R2 发送更新包过来, R1 用接收接口的子网掩码来对待这条路由, 所以出现了 192.168.1.128/30。如果此时查看 R2 的路由表, 会发现有如下显示:

```

R2#show ip route
192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
C    192.168.1.64/30 is directly connected, Serial1/0
R    192.168.1.0/26 [120/1] via 192.168.1.65, 00:01:21, Serial1/0
C    192.168.1.128/26 is directly connected, Loopback0

```

这时却没有多出一条 “R 192.168.1.0/30” 的路由, 这是因为 R2 是后改的 S1/0 接口子网掩码, 当 R1 发现要传送出去的路由 “/26” 与外出接口的网络位 “/30” 不相同, R1 不发送不一致的主类网络路由更新。也就是说, 自从 R1 更改了子网掩码后, 没有发出任何一条不一致的主类网络更新, 其实 R2 更改了子网掩码后, 也没有发出任何不一致的主类网络更新, 之前发送的一条是在没有更改子网掩码之前。有关这一点, 可以在两台路由器上使用 “debug ip rip” 命令, R1 上的显示如下:

```

*Mar 1 01:41:22.715: RIP: sending v1 update to 255.255.255.255 via Serial1/1 (192.168.1.65)
*Mar 1 01:41:22.719: RIP: build update entries - suppressing null update

```

R1 抑制了空的更新, 也就是说, R1 没有发出任何更新。R2 的显示与此类似, 既然路由没有更新了, 路由表中的条目慢慢就会老化, 下面是稍后在 R1 上显示的路由表。

```

R1#show ip route
Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C    192.168.1.64/30 is directly connected, Serial1/1
C    192.168.1.0/26 is directly connected, Loopback0
R    192.168.1.128/30 [120/1] via 192.168.1.66, 00:02:58, Serial1/1
R    192.168.1.128/26 is possibly down,
    routing via 192.168.1.66, Serial1/1

```

从上面的输出中, 可以看到路由 “R 192.168.1.128/26” 已经是失效路由了 (possibly down), “R 192.168.1.128/30” 存在的时间也接近了失效时间。再等一会, 或者在路由器上执行 “clear ip route *” 命令清除路由表, 使路由器重新学习新的路由, 这样过时的信息就会被手工删除, 而不用等刷新定时器到达, 在路由器 R1 上查看路由表, 显示如下:

```

R1#show ip route
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.64/30 is directly connected, Serial1/1
C    192.168.1.0/26 is directly connected, Loopback0

```

从上面的输出中, 可以看到 R1 和 R2 在 VLSM 的环境下, 彼此学不到对方的路由, 也就是说, RIPv1 不支持 VLSM。

综上所述, RIPv1 是一个有类路由协议, 不是说 RIPv1 不能支持带子网的网络地址 (图 6-4-2 就可以), 但一定要是连续的 (不能被其他主类网络地址分割, 图 6-4-1 被分割了)、子网掩码长度都相同 (非 VLSM, 图 6-4-3 使用了 VLSM) 的网络。

6.4.2 RIPv2 的增强特性**

RIP 经过若干年的发展, 从一个有类路由选择协议——RIPv1 改进到了无类路由选择协议——RIPv2。RIPv2 是从 RIPv1 升级而来的, 和 RIPv1 有很多相似的特性:

- 也用跳数作为度量值, 最大值为 15。
- 也是距离矢量的路由选择协议。
- 也容易产生路由环路, 使用最大跳计数、水平分割、触发更新、路由中毒和抑制定时器来防止路由环路。
- 也是周期性更新, 默认每 30 秒发送一次路由更新。

但 RIPv2 是 RIPv1 的增强版, 具有以下增强特性:

- 在路由更新中, 携带有子网掩码的路由选择信息, 因此 RIPv2 支持 VLSM 和 CIDR。
- 提供身份验证功能, 支持明文和 MD5 验证。
- 在路由更新信息中包含下一跳路由器的 IP 地址。
- 使用外部路由标记 (external route tags), 路由重发布时, 外部路由标记很有用, 路由重发布属于 CCNP 部分的知识点。
- 使用组播更新取代版本 1 的广播更新, 路由更新的效率更高。
- 可以关闭自动汇总, 并支持手工汇总。

6.4.3 RIPv2 的配置**

1. RIPv2 基本配置

RIPv2 的基本配置与 RIPv1 类似, 配置的命令格式如下:

```
Router(config)#router rip           启动RIP路由选择进程。
Router(config-router)#version 2     使用RIPv2, 如不使用该命令, 默认使用的是RIPv1。
Router(config-router)#network 主类网络号
宣告直连的主类网络, 这里和RIPv1相同。尽管RIPv2支持VLSM, 可在宣告网络的时候, 添加的仍然是主类网络地址。
```

2. RIPv2 支持 VLSM

这里使用 RIPv2 完成如图 6-4-3 所示的配置, R1 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 192.168.1.65 255.255.255.252
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ip add 192.168.1.1 255.255.255.192
R1(config-if)#router rip
R1(config-router)#version 2         声明版本2。
R1(config-router)#net 192.168.1.0   加入直连的主类网络号。
```

R2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 192.168.1.66 255.255.255.252
R2(config-if)#no shut
R2(config-if)#int lo0
```



```
R2(config-if)#ip add 192.168.1.130 255.255.255.192
R2(config-if)#router rip
R2(config-router)#ver 2
R2(config-router)#net 192.168.1.0
```

查看 R1 的路由表，并测试网络的连通性，显示如下：

```
R1#show ip route
 192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
C    192.168.1.64/30 is directly connected, Serial1/1
C    192.168.1.0/26 is directly connected, Loopback0
R    192.168.1.128/26 [120/1] via 192.168.1.66, 00:00:00, Serial1/1
R1#ping 192.168.1.130

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.130, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/18/32 ms
```

从上面的输出中可以得出结论，RIPv2 支持 VLSM。不要关闭实验机架，继续往下阅读。

3. 使用“debug ip rip”命令查看输出信息

在路由器 R1 上使用“debug ip rip”命令，显示如下：

```
R1#debug ip rip
RIP protocol debugging is on
R1#
*Mar 1 00:25:40.283: RIP: sending v2 update to 224.0.0.9 via Serial1/1 (192.168.1.65)
*Mar 1 00:25:40.287: RIP: build update entries
*Mar 1 00:25:40.287:   192.168.1.0/26 via 0.0.0.0, metric 1, tag 0
*Mar 1 00:25:50.303: RIP: received v2 update from 192.168.1.66 on Serial1/1
*Mar 1 00:25:50.307:   192.168.1.128/26 via 0.0.0.0 in 1 hops
```

从上面的输出中可以看到，发送的是版本 2 的更新“sending v2 update”；版本 2 使用的是组播更新，组播地址是“224.0.0.9”；版本 2 发送的路由更新信息中携带了子网掩码的长度“192.168.1.0/26”；版本 2 发送的路由更新信息中包括了下一跳的地址“via 0.0.0.0”；版本 2 使用了路由标记“tag 0”。

4. RIPv2 支持 CIDR

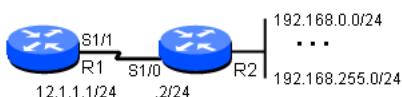


图 6-4-4 CIDR

在图 6-4-4 中，路由器 R2 有很多 192.168.*.0/24 的网络，如何在 RIPv2 中以 CIDR 的方式把路由宣告出去呢？这里的配置仅仅是演示 RIPv2 支持 CIDR，具体配置不要求 CCNA 考生掌握。

R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#router rip
R1(config-router)#version 2
R1(config-router)#net 12.0.0.0
```

R2 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#ip route 192.168.0.0 255.255.0.0 null 0
配置这句话的目的是在路由器上生成 192.168.0.0/16 的路由。
```

```
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#router rip
R2(config-router)#version 2
R2(config-router)#net 12.0.0.0
R2(config-router)#redistribute static
```

因RIP只能宣告主类的网络，无法宣告CIDR的超网，这里使用的方法是重发布，可以重发布一个超网进来。

在路由器R1上查看路由表，显示如下：

```
R1#show ip route
 12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/1
R    192.168.0.0/16 [120/1] via 12.1.1.2, 00:00:18, Serial1/1
```

从上面的输出中可以看到，R1可以通过RIPv2学到“R 192.168.0.0/16”超网路由，这证明RIPv2支持CIDR。在R1和R2上，使用“version 1”，改成RIPv1，使用“clear ip route *”命令清除过时的路由表，使用路由器重新学习路由。再次在R1上查看路由表，显示如下：

```
R1#show ip route
 12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/1
```

从上面的输出中，看不到192.168.0.0/16的RIP路由，这证明RIPv1不支持CIDR。

5. RIPv2路由的手工汇总

RIPv1和RIPv2都会在主类网络的边界自动汇总，区别在于RIPv2的自动汇总可以关闭，并支持手工汇总，RIPv1的自动汇总不可以关闭。

使用RIPv2完成如图6-4-1所示的配置。在前面版本1配置的基础上添加“version 2”改成版本2，在路由器R2上查询路由表，结果显示的和版本1的结果相同。这是因为路由器R1和R3向R2发送路由更新的时候，在R1的S1/1接口和R3的S1/0接口（192.168.1.0主类网络的边界）执行了路由的自动汇总。

在路由器R1、R2、R3上使用下面的命令关闭自动汇总。

```
R1(config)#router rip
R1(config-router)#ver 2
R1(config-router)#no auto-summary
```

只有RIPv2才能关闭自动汇总。

关闭自动汇总之后，路由器在主类网络的边界将不再自动汇总。

三台路由器都配置完成后，先清除过时的路由表条目，然后在R1、R2、R3上分别查看路由表，R1显示如下：

```
R1(config-router)#do show ip route
 23.0.0.0/24 is subnetted, 1 subnets
R    23.1.1.0 [120/1] via 12.1.1.2, 00:00:01, Serial1/1
 12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/1
 192.168.1.0/25 is subnetted, 2 subnets
C    192.168.1.0 is directly connected, Loopback0
R    192.168.1.128 [120/2] via 12.1.1.2, 00:00:02, Serial1/1
```

R2显示如下：

```
R2#sho ip route
 23.0.0.0/24 is subnetted, 1 subnets
C    23.1.1.0 is directly connected, Serial1/1
 12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/0
 192.168.1.0/25 is subnetted, 2 subnets
```

```

R      192.168.1.0 [120/1] via 12.1.1.1, 00:00:03, Serial1/0
R      192.168.1.128 [120/1] via 23.1.1.3, 00:00:03, Serial1/1

```

R3 显示如下:

```

R3#show ip route
 23.0.0.0/24 is subnetted, 1 subnets
C    23.1.1.0 is directly connected, Serial1/0
 12.0.0.0/24 is subnetted, 1 subnets
R    12.1.1.0 [120/1] via 23.1.1.2, 00:00:23, Serial1/0
 192.168.1.0/25 is subnetted, 2 subnets
R    192.168.1.0 [120/2] via 23.1.1.2, 00:00:23, Serial1/0
C    192.168.1.128 is directly connected, Loopback0

```

从上面的输出中, 可以看出关闭自动汇总后, **RIPv2** 可以支持不连续的子网。关闭自动汇总后, 也会带来新的问题, 路由表变大了, 在图 6-4-5 中, 如果不关闭自动汇总, 将会造成路由可达性问题; 如果关闭自动汇总, 路由器 R1 将向其他路由器通告 4 条明细的路由, 使路由表变大。解决的办法就是使用 **RIPv2** 的手工汇总。

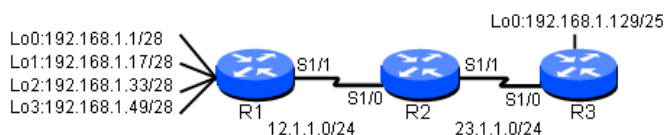


图 6-4-5 手工汇总

R1 的配置如下:

```

Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ip add 192.168.1.1 255.255.255.240
R1(config-if)#int lo1
R1(config-if)#ip add 192.168.1.17 255.255.255.240
R1(config-if)#int lo2
R1(config-if)#ip add 192.168.1.33 255.255.255.240
R1(config-if)#int lo3
R1(config-if)#ip add 192.168.1.49 255.255.255.240
R1(config-if)#router rip
R1(config-router)#version 2
R1(config-router)#net 12.0.0.0
R1(config-router)#net 192.168.1.0
R1(config-router)#no auto-summary

```

R2 的配置如下:

```

Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#router rip
R2(config-router)#ver 2
R2(config-router)#net 12.0.0.0
R2(config-router)#net 23.0.0.0
R2(config-router)#no auto

```

R3 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo0
R3(config-if)#ip add 192.168.1.129 255.255.255.128
R3(config-if)#router rip
R3(config-router)#ver 2
R3(config-router)#net 23.0.0.0
R3(config-router)#net 192.168.1.0
R3(config-router)#no auto
```

配置完成后, 查看 R2 的路由表, 显示如下:

```
R2#show ip route
 23.0.0.0/24 is subnetted, 1 subnets
C    23.1.1.0 is directly connected, Serial1/1
 12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/0
 192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
R    192.168.1.32/28 [120/1] via 12.1.1.1, 00:00:27, Serial1/0
R    192.168.1.48/28 [120/1] via 12.1.1.1, 00:00:27, Serial1/0
R    192.168.1.0/28 [120/1] via 12.1.1.1, 00:00:27, Serial1/0
R    192.168.1.16/28 [120/1] via 12.1.1.1, 00:00:27, Serial1/0
R    192.168.1.128/25 [120/1] via 23.1.1.3, 00:00:01, Serial1/1
```

从上面的输出中, 可以看到 R2 从 R1 上学到了 192.168.1.0/28、192.168.1.16/28、192.168.1.32/28、192.168.1.48/28, 共 4 条明细路由。关闭自动汇总后, 可以在 R1 上使用下面的命令进行手工汇总:

```
R1(config)#int s1/1
R1(config-if)#ip summary-address rip 192.168.1.0 255.255.255.192
```

在向外发送路由的接口进行汇总, 如果路由器 R1 有多个外出接口, 在每个外出接口都需要进行汇总。

R1 上汇总完成后, 清除 R2 上过时的路由表, 稍后显示 R2 上最新的路由表, 显示如下:

```
R2#show ip route
 23.0.0.0/24 is subnetted, 1 subnets
C    23.1.1.0 is directly connected, Serial1/1
 12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/0
 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
R    192.168.1.0/26 [120/1] via 12.1.1.1, 00:00:04, Serial1/0
R    192.168.1.128/25 [120/1] via 23.1.1.3, 00:00:04, Serial1/1
```

从上面的输出中, 可以发现 R1 只向 R2 通告一条汇总后的路由。

6. 路由翻动 (Route Flapping)

当路由器接口在“UP”和“DOWN”状态之间快速变换时就会产生路由翻动。路由翻动可能是由很多原因引起的, 包括端口故障或端接不良的介质。路由汇总除了可以减小路由表大小外, 还可以有效地将上游路由器从路由翻动问题中隔离出来。在图 6-4-5 中, 路由没有手工汇总前, 不停地关闭和打开 R1 的 Loopback 0 接口, 来模拟路由的翻动, R1 上路由的翻动将会引起 R2 和 R3 接收新的路由更新信息, 它们的处理器必须投入工作, 影响整个网络的性能。

R1 上采用手工路由汇总后, 再不停地关闭和打开 R1 的 Loopback 0 接口, R1 的直连路由虽然不停地发生变化, 但 R1 的汇总路由没有发生变化, R2 和 R3 可以从 R1 的路由翻动中解脱出来。

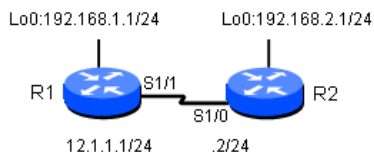


图 6-4-6 RIPv2 验证

7. RIPv2 路由验证

RIPv2 支持验证，通过配置验证，可以保障路由器间的可靠更新。配置图 6-4-6 中的 RIPv2 验证，保障路由器 R1 和 R2 之间的可靠路由更新。

使用下面的命令配置 RIPv2 的验证模式：

```
R1(config)#int s1/1
R1(config-if)#ip rip authentication mode ?
md5      Keyed message digest
text     Clear text authentication

R1(config-if)#ip rip authentication mode md5
```

可以看出 RIPv2 可以支持 text 和 MD5 两种验证模式，text 验证将会在网上以明文发送密码，安全性不高，建议使用 MD5 验证。

使用下面的命令配置密钥链：

```
R1(config)#key chain test
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco
```

配置密钥链的名称是 test，密钥链中 key 1 的密钥是 cisco。在路由器上可以配置多个密钥链，一个密钥链中也可以配置多个 key，不同的 key 可以使用不同的密钥。因为 CCNA 考试中对 RIPv2 的验证不做过多要求，这里就不深入讨论它们的组合了。读者在两端使用相同的配置即可。

在路由器接口下调用密钥链：

```
R1(config)#int s1/1
R1(config-if)#ip rip authentication key-chain test
```

下面配置 R1 和 R2 之间的 MD5 验证，使用的密钥是 cisco。R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#router rip
R1(config-router)#ver 2
R1(config-router)#net 12.0.0.0
R1(config-router)#net 192.168.1.0
R1(config-router)#exit
R1(config)#key chain ccna 创建密钥链 ccna，验证双方配置的密钥链名称可以不一样。
R1(config-keychain)#key 1 配置密钥链 ccna 中的 key 1。
R1(config-keychain-key)#key-string cisco 配置密码串。
R1(config-keychain-key)#int s1/1
R1(config-if)#ip rip authentication mode md5 验证的模式是 MD5。
R1(config-if)#ip rip authentication key-chain ccna 调用的验证密钥链是 ccna。
```

R2 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int lo0
R2(config-if)#ip add 192.168.2.1 255.255.255.0
```

```
R2(config-if)#router rip
R2(config-router)#ver 2
R2(config-router)#net 12.0.0.0
R2(config-router)#net 192.168.2.0
R2(config-router)#exit
R2(config)#key chain ccna
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco
R2(config-keychain-key)#int s1/0
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain ccna
```

在两台路由器上使用“show ip route”命令，可以发现 R1 和 R2 均可正确地学到对方的路由。读者可以把两端配置成不同的密码，来检验路由能否正常交互。

8. RIPv1 和 RIPv2 的共存

为了锻炼读者的排错能力，本知识点以排错的形式出现。CCNA 模拟机架中路由器 R1 和 R2 的 IP 地址分配如图 6-4-6 所示，R1 和 R2 的配置在光盘中的“配置\6\1”文件夹下，请读者把 R1 和 R2 的配置文件复制进来。具体做法是：复制 R1.txt 中的文本，进入路由器 R1 的全局配置模式下，粘贴即可，屏幕显示如下：

```
Router(config)#version 12.4
Router(config)#service timestamps debug datetime msec
Router(config)#service timestamps log datetime msec
Router(config)#no service password-encryption
Router(config)#!
Router(config)#hostname R1
R1(config)#!
R1(config)#boot-start-marker
R1(config)#boot-end-marker
R1(config)#!
R1(config)#!
R1(config)#no aaa new-model
R1(config)#!
R1(config)#ip cef
R1(config)#!
R1(config)#!
R1(config)#interface Loopback0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)#!
R1(config-if)#interface FastEthernet0/0
R1(config-if)# no ip address
R1(config-if)# shutdown
R1(config-if)# duplex auto
R1(config-if)# speed auto
R1(config-if)#!
R1(config-if)#interface Serial1/0
R1(config-if)# no ip address
R1(config-if)# shutdown
R1(config-if)# serial restart-delay 0
R1(config-if)#!
R1(config-if)#interface Serial1/1
R1(config-if)# ip address 12.1.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# serial restart-delay 0
R1(config-if)#!
R1(config-if)#interface Serial1/2
R1(config-if)# no ip address
R1(config-if)# shutdown
R1(config-if)# serial restart-delay 0
R1(config-if)#!
R1(config-if)#interface Serial1/3
R1(config-if)# no ip address
```

```

R1(config-if)# shutdown
R1(config-if)# serial restart-delay 0
R1(config-if)#!
R1(config-if)#interface FastEthernet2/0
R1(config-if)# no ip address
R1(config-if)# shutdown
R1(config-if)# duplex auto
R1(config-if)# speed auto
R1(config-if)#!
R1(config-if)#router rip
R1(config-router)# version 2
R1(config-router)# network 12.0.0.0
R1(config-router)# network 192.168.1.0
R1(config-router)#!
R1(config-router)#no ip http server
R1(config)#no ip http secure-server
R1(config)#!
R1(config)#!
R1(config)#control-plane
R1(config-cp)#!
R1(config-cp)#!
R1(config-cp)#!
R1(config-cp)#line con 0
R1(config-line)#line aux 0
R1(config-line)#line vty 0 4
R1(config-line)#!
R1(config-line)#!
R1(config-line)#end
R1#

```

路由器 R2 上执行同样的操作，完成路由器的配置。读者可以借鉴这种方法恢复路由器的配置：使用“show running-config”命令查看路由器的运行配置文件，然后把内容复制下来，存为文本文件的格式，以后若不小心丢失了路由器配置文件，可以复制备份的文本文件，再粘贴回路由器。使用这种方法，一定要特别注意，这里粘贴的文件和正在运行的配置文件是合并的，而不是覆盖的。正在运行的接口下默认都是“shutdown”，备份的文件中都使用了“no shut”操作，可“no shut”在备份文件中是隐藏的，结果两个文件合并后，接口还是 shutdown 的，一般的操作就是进入那些需要使用的接口，使用“no shut”命令打开接口，或者修改保存的备份配置文件，在里面加入“no shut”命令。本例使用的方法就是修改了保存的备份配置文件。本书后面还会以这样的形式出现一些实验配置或排错题。

查看路由器 R1 的路由表，显示如下：

```

R1#show ip route
      12.0.0.0/24 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, Serial1/1
C       192.168.1.0/24 is directly connected, Loopback0

```

查看路由器 R2 的路由表，显示如下：

```

R2#show ip route
      12.0.0.0/24 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, Serial1/0
R       192.168.1.0/24 [120/1] via 12.1.1.1, 00:00:14, Serial1/0
C       192.168.2.0/24 is directly connected, Loopback0

```

从上面的输出中，可以看到 R2 学到了 R1 上的路由，可是 R1 却没有学到 R2 上的路由。在路由器 R2 上执行“show run | b r r”命令，该命令是“Show running-config | begin router rip”的简写格式，“|”是过滤符号，“begin router rip”表示从 router rip 开始显示配置。显示如下：

```

R2#show run | b r r
router rip
network 12.0.0.0
network 192.168.2.0

```


省略部分输出。

从上面的输出中，可以看到 R2 宣告了 192.168.2.0 网络。进一步在 R1 上使用“debug ip rip”命令查看 R2 有没有路由发送过来，可以看到这样的输出：“ignored v1 packet from 12.1.1.2 (illegal version)”，提示从 R2 收到了版本 1 的数据包不合法，R1 忽略 R2 发过来的路由更新。既然两端的版本不匹配，可是 R2 为何可以学到 R1 上的路由呢？在 R1 上使用“show ip protocols”命令，显示如下：

```
R1#show ip protocols
省略部分输出。
Default version control: send version 2, receive version 2
Interface      Send Recv  Triggered RIP  Key-chain
Serial1/1      2         2
Loopback0     2         2
```

在 R2 上使用“show ip protocols”命令，显示如下：

```
R2#show ip protocols
省略部分输出。
Default version control: send version 1, receive any version
Interface      Send Recv  Triggered RIP  Key-chain
Serial1/0      1         1 2
Loopback0     1         1 2
```

从上面的输出中，可以发现 R1 发送版本 2，接收版本 2；而 R2 发送版本 1，接收版本 1 和版本 2。至此，找到两端路由不对称的原因了，可以把 R2 的 RIP 协议也更改成版本 2；也可以使用下面的命令，让 R2 也发送版本 2，或者让 R1 也接收版本 1。配置接口收发 RIP 版本的命令如下：

```
R1(config)#int s1/1
R1(config-if)#ip rip receive version 1 2
```

或者

```
R2(config)#int s1/0
R2(config-if)#ip rip send version 1 2
```

再次在 R1 上查看路由表，发现可以正常学到 R2 上的路由了。

6.4.4 常见路由协议的比较**

为了便于读者正确区分一些常用路由协议的特征，表 6-4-1 对它们进行了比较。

表 6-4-1 路由协议对比表

	RIPv1	RIPv2	IGRP	EIGRP	OSPF
收敛速度	慢	慢	慢	很快	快
网络规模	小	小	小	大	很大
VLSM	不支持	支持	不支持	支持	支持
CIDR	不支持	支持	不支持	支持	支持
资源占用	低	低	低	中	高
配置和维护	简单	简单	简单	中	复杂
类型	距离矢量	距离矢量	距离矢量	高级距离矢量	链路状态
自动汇总	不可关闭	可关闭	不可关闭	可关闭	没有自动汇总
手工汇总	不支持	支持	不支持	支持	支持
路由验证	不支持	支持	不支持	支持	支持
更新方式	周期性广播更新	周期性组播更新	周期性广播更新	触发式组播更新	触发式组播更新



6.5 路由查找***

本节介绍路由表的结构和路由的查找过程。作为一名网络管理员深入地了解路由表结构和路由的查找过程，有助于诊断和排除路由表的问题。例如可能会遇到这种情况，路由表和预期的一样，但数据包的转发却和预期的不一样。本节涉及 CCNA 考试的知识点是路由无类（ip classless）查找和有类（no ip classless）查找的区别。

6.5.1 路由表结构**

配置如图 6-5-1 中所示的路由器 R1 和 R2。

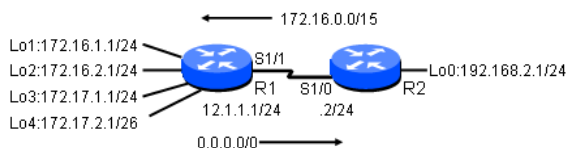


图 6-5-1 路由表结构

R1 配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int lo1
R1(config-if)#ip add 172.16.1.1 255.255.255.0
R1(config-if)#int lo2
R1(config-if)#ip add 172.16.2.1 255.255.255.0
R1(config-if)#int lo3
R1(config-if)#ip add 172.17.1.1 255.255.255.0
R1(config-if)#int lo4
R1(config-if)#ip add 172.17.2.1 255.255.255.192
R1(config-if)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.2
```

R2 配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int lo0
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip route 172.16.0.0 255.254.0.0 12.1.1.1
```

它们的路由表结构是什么样的呢？在路由器 R1 上查看路由表，显示如下：

```
R1#show ip route
172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.17.1.0/24 is directly connected, Loopback3
C    172.17.2.0/26 is directly connected, Loopback4
172.16.0.0/24 is subnetted, 2 subnets
C    172.16.1.0 is directly connected, Loopback1
C    172.16.2.0 is directly connected, Loopback2
12.0.0.0/24 is subnetted, 1 subnets
```

```
C      12.1.1.0 is directly connected, Serial1/1
S*    0.0.0.0/0 [1/0] via 12.1.1.2
```

在路由器 R2 上查看路由表，显示如下：

```
R2#show ip route
      12.0.0.0/24 is subnetted, 1 subnets
C      12.1.1.0 is directly connected, Serial1/0
C    192.168.2.0/24 is directly connected, Loopback0
S    172.16.0.0/15 [1/0] via 12.1.1.1
```

这里先看路由器 R2 上的显示，为何 192.168.2.0/24 和 172.16.0.0/15 只显示了一行，而 12.1.1.0/24 却显示成两行？这里首先要知道级别 1（Level 1）路由和级别 2（Level 2）路由。

（1）级别 1 路由（Level 1 route）

级别 1 路由是指一条路由使用的子网掩码小于或等于有类网络默认的网络掩码。级别 1 的路由包括：

- **网络路由**：一条路由使用的子网掩码等于有类网络的子网掩码，比如 R2 上的 192.168.2.0/24。
- **超网路由**：一条路由使用的子网掩码小于有类网络的子网掩码，比如 R2 上的 172.16.0.0/15。
- **默认路由**：0.0.0.0/0，比如 R1 上的 0.0.0.0/0。

上面列出的 3 种级别 1 的路由都只显示成一行。

（2）父路由（Parent route）

注意路由器 R2 的路由表的第一行，12.0.0.0/24 就是一条父路由，父路由不包括下一跳的 IP 地址或路由器的外出接口。父路由实际上是一个头部，暗示后面会有级别 2 的路由，级别 2 的路由也称为子路由（Child route）。无论什么时候只要路由表中出现一条子网掩码长度大于有类网络子网掩码长度的路由，父路由就会被自动创建。

路由器 R2 的路由表中“12.0.0.0/24 is subnetted, 1 subnets”表示的是父路由，有子网被创建，子网掩码的位数是 24，该主类网络在路由表中有一个子网。

路由器 R1 的路由表中“172.17.0.0/16 is **variably** subnetted, 2 subnets, 2 masks”表示的也是父路由，因为不同的子路由掩码长度不同，所以父路由中的掩码长度是默认主类网络的掩码，“**variably subnetted**”显示是变长子网，有两个子网，有两种掩码。不同的子网掩码在子路由中分别表示。

路由器 R1 的路由表中“172.16.0.0/24 is subnetted, 2 subnets”表示的也是父路由，因为两个子路由的掩码长度相同，所以父路由中用“/24”直接表示。父路由中已经表示出了掩码长度，子路由中就不用再表示掩码长度了。

注意：父路由也属于级别 1 的路由，归为级别 1 中的网络路由一类。

（3）子路由（Child route），也称为级别 2 路由（Level 2 route）

子路由和级别 2 路由是同一个意思，子路由包括了下一跳路由器的 IP 地址或本路由器的外出接口。如果所有子路由的掩码长度相同，相同的掩码长度将在父路由中体现出来，子路由中就不再出现掩码长度了，如路由器 R1 中的“C 172.16.1.0 is directly connected, Loopback1”和“C 172.16.2.0 is directly connected, Loopback2”；如果所有子路由的掩码长度不同，子网掩码的长度将在各个子路由中表现出来，如路由器 R1 中的“C 172.17.1.0/24 is directly connected, Loopback3”和“C 172.17.2.0/26 is directly connected, Loopback4”。

(4) 最终路由 (Ultimate Route)

所谓的最终路由,就是路由条目中包括下一跳路由器的 IP 地址或本路由器的外出接口。除父路由外的所有级别 1 和级别 2 路由(也就是子路由)都是最终路由。

6.5.2 路由查找过程***

当路由器接收到一个 IP 报文时,检查目的 IP 地址,查找路由表。路由器是如何决定哪一条路由是最佳路由的?子网掩码在路由查找过程中有什么影响?如果在路由表中没有找到好的匹配,是否要使用超网路由或默认路由?带着这些问题,来学习路由的查找过程。

路由查找过程如下:

① 路由器根据数据包中的目的 IP 地址,查找级别 1 路由:网络路由(包括父路由)、超网路由和默认路由。

② 如果最佳匹配(指的是最长子网掩码匹配)是级别 1 的最终路由(路由条目中包括下一跳路由器的 IP 地址或本路由器的外出接口,除父路由外的级别 1 和级别 2 路由都是最终路由),这条路由被用来转发数据包。

③ 如果最佳匹配是级别 1 中的父路由,继续下一步查找。

④ 路由器在级别 1 的父路由中找到了匹配,继续查找该父路由的子路由。

⑤ 如果有一条子路由匹配,这条子路由被用来转发数据包。

⑥ 如果子路由中没有找到匹配,继续下一步查找。

⑦ 判断路由器执行的是有类还是无类路由行为(routing behavior)。这里的有类和无类路由行为与有类和无类路由协议不同。有类和无类路由协议影响路由表的建立,而有类和无类路由行为是在路由表建立后决定怎样搜索路由表。有类和无类路由行为是通过 ip classless 和 no ip classless 命令来改变的。如果是有类路由行为(no ip classless)则跳到⑧,如果是无类路由行为(ip classless)则跳到⑨。

⑧ 有类路由行为:终止查找,丢弃数据包。

⑨ 无类路由行为:继续查找级别 1 的超网路由和默认路由,使用超网路由或默认路由转发数据包。

⑩ 如果没有找到超网路由,路由器也没有配置默认路由,则终止查找,丢弃数据包。

上面路由的查找过程比较复杂,读者没有必要记住所有的步骤,只要能正确判断数据包如何转发就行了。这里针对路由的查找过程,举几个例子。

 **例 1:** 在图 6-5-1 中, R1 去往 2.2.2.2 的数据包。

路由器 R1 执行查找过程,① 查找级别 1 的路由。② 找到了最佳匹配 0.0.0.0/0,这是一条最终路由,下一跳是 12.1.1.2, R1 把数据包发往路由器 R2。在 R2 上配置 Loopback 1 接口的 IP 地址为 2.2.2.2/24。在 R1 上 ping 2.2.2.2, 显示如下:

```
R1#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/13/24 ms
```

从上面的输出可以看到, R1 可以成功到达 2.2.2.2。

 **例 2:** 在图 6-5-1 中, R1 去往 12.1.1.2 的数据包。


路由器 R1 执行查找过程,① 查找级别 1 的路由。② 找到了最佳匹配 12.0.0.0/24, 这

不是一条最终路由。③ 这条是级别 1 的父路由。④ 继续查找该父路由的子路由。⑤ 子路由中的 12.1.1.0 匹配 12.1.1.2, R1 从 S1/1 接口把数据包转发出去。R1 成功地收到了应答包。R1 显示如下:

```
R1#ping 12.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/21/40 ms
```

从上面的输出可以看到, R1 可以成功到达 12.1.1.2。

 **例 3:** R1 去往 172.16.3.1 的数据包。

! **注意:** 因为思科路由器默认使用的是快速交换, 快速交换的使用会得出和前面叙述不一致的结论。开始测试前, 在路由器 R1 上使用 `no ip cef` 关闭快速交换, 使用进程交换。

前面的查找过程与例 2 类似, 接下来查找到: ⑥ 子路由中没有找到匹配。⑦ 看路由器 R1 执行的是有类还是无类路由行为。⑧ 在路由器 R1 上使用下面的命令, 让路由器 R1 执行有类路由行为:

```
R1(config)#no ip cef
R1(config)#no ip classless
```

在 R2 上配置 Loopback 2 接口的 IP 地址为 172.16.3.1/24。在 R1 上 ping 172.16.3.1, 显示如下:

```
R1#ping 172.16.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

从上面的输出可以看到, R1 无法到达 172.16.3.1。

⑨ 在路由器 R1 上使用下面的命令, 让路由器 R1 执行无类路由行为:

```
R1(config)#ip classless
```

因为 `ip classless` 是默认配置, `show run` 的时候看不到该配置。现在路由器 R1 执行无类路由行为, 找不到子网路由后, 继续查找级别 1 的路由, 发现有默认路由, 使用默认路由对数据包进行转发。继续在路由器 R1 上 ping 172.16.3.1, 显示如下:

```
R1#ping 172.16.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/12 ms
```

从上面的输出可以看到, R1 可以成功到达 172.16.3.1 了。



6.6 真题精选***

1. Refer to the exhibit. After a RIP route is marked invalid on Router_1, how much time will elapse before that route is removed from the routing table?

```

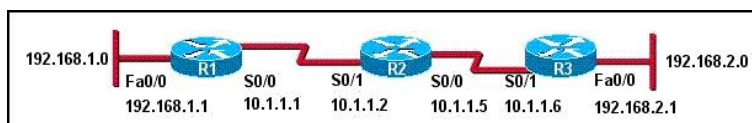
Router_1# show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 8 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  <output omitted>

Router_1#

```

- A. 30 seconds B. 60 seconds C. 90 seconds
D. 180 seconds E. 240 seconds

2. Refer to the exhibit. The network shown in the exhibit is running the RIPv2 routing protocol. The network has converged, and the routers in this network are functioning properly. The FastEthernet0/0 interface on R1 goes down. In which two ways will the routers in this network respond to this change? (Choose two.)



- A. All routers will reference their topology database to determine if any backup routes to the 192.168.1.0 network are known.
B. Routers R2 and R3 mark the route as inaccessible and will not accept any further routing updates from R1 until their hold-down timers expire.
C. Because of the split-horizon rule, router R2 will be prevented from sending erroneous information to R1 about connectivity to the 192.168.1.0 network.
D. When router R2 learns from R1 that the link to the 192.168.1.0 network has been lost, R2 will respond by sending a route back to R1 with an infinite metric to the 192.168.1.0 network.
E. R1 will send LSAs to R2 and R3 informing them of this change, and then all routers will send periodic updates at an increased rate until the network again converges.

3. Which of the following are true regarding the command output shown in the display? (Choose two.)

```

RtrA#debug ip rip
RIP protocol debugging is on
RtrA#
1d05h: R.IP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (172.16.1.1)
1d05h: R.IP: build update entries
1d05h: network 10.0.0.0 metric 1
1d05h: network 192.168.1.0 metric 2
1d05h: R.IP: sending v1 update to 255.255.255.255 via Serial0/0 (10.0.8.1)
1d05h: R.IP: build update entries
1d05h: network 172.16.0.0 metric 1
RtrA#
1d05h: R.IP: received v1 update from 10.0.15.2 on Serial0/0
1d05h: 192.168.1.0 in 1 hops
1d05h: 192.168.168.0 in 16 hops (inaccessible)

```

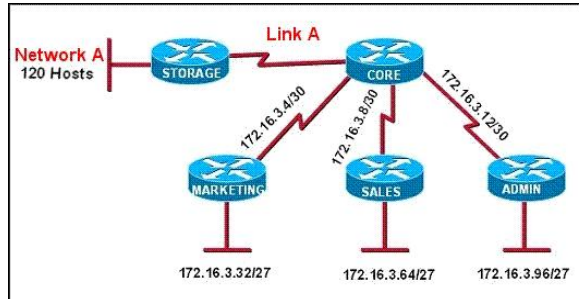
- A. There are at least two routers participating in the RIP process.
B. A ping to 192.168.168.2 will be successful.
C. A ping to 10.0.15.2 will be successful.

D. RtrA has three interfaces participating in the RIP process.

4. In the implementation of VLSM techniques on a network using a single Class C IP address, which subnet mask is the most efficient for point-to-point serial links?

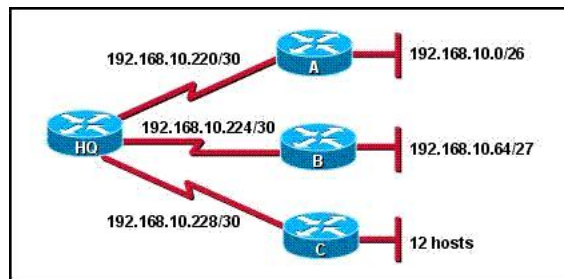
- A. 255.255.255.0 B. 255.255.255.240 C. 255.255.255.248
D. 255.255.255.252 E. 255.255.255.254

5. Refer to the exhibit. All of the routers in the network are configured with the ip subnet-zero command. Which network addresses should be used for Link A and Network A? (Choose two.)



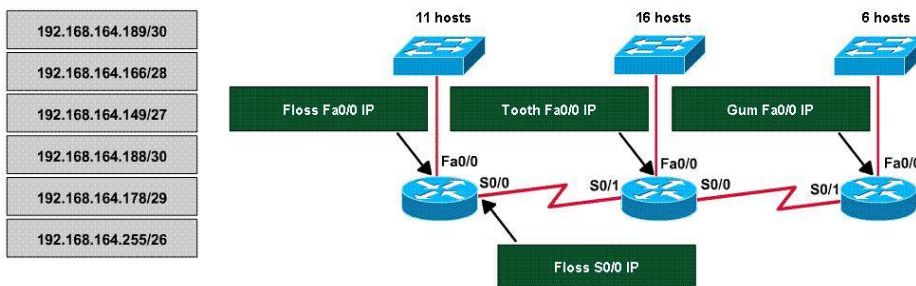
- A. Network A - 172.16.3.48/26 B. Network A - 172.16.3.128/25
C. Network A - 172.16.3.192/26 D. Link A - 172.16.3.0/30
E. Link A - 172.16.3.40/30 F. Link A - 172.16.3.112/30

6. Refer to the exhibit. A new subnet with 12 hosts has been added to the network. Which subnet address should this network use to provide enough useable addresses while wasting the fewest addresses?



- A. 192.168.10.80/28 B. 192.168.10.80/29
C. 192.168.10.96/28 D. 192.168.10.96/29

7. A dental firm is redesigning the network that connects its three locations. The administrator gave the networking team 192.168.164.0 to use for addressing the entire network. After subnetting the address, the team is ready to assign the addresses. The administrator plans to configure ip subnet-zero and use RIP v2 as the routing protocol. As a member of the networking team, you must address the network and at the same time conserve unused addresses for future growth. With those goals in mind, drag the host addresses on the left to the correct router interface. Once one of the routers is partially configured. Move your mouse over a router to view its configuration. Not all of the host addresses on the left are necessary.



Drag and drop question. Drag the items to the proper locations.

8. Which three statements are correct about RIP version 2? (Choose three.)

- A. It has the same maximum hop count as version 1.
- B. It uses broadcasts for its routing updates.
- C. It is a classless routing protocol.
- D. It has a lower default administrative distance than RIP version 1.
- E. It supports authentication.
- F. It does not send the subnet mask in updates.

9. Refer to the exhibit. What can be determined about routes that are learned from the router at IP address 190.171.23.12?

```
HQ_Router# show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 18 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface        Send Recv  Triggered RIP  Key-chain
    Ethernet0         2       2
    Ethernet1         2       2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    190.171.0.0
    190.172.0.0
  Routing Information Sources:
    Gateway         Distance   Last Update
    190.171.23.10    120       00:00:22
    190.171.23.12    120       00:03:30
    190.172.32.10    120       00:00:16
  Distance: (default is 120)

HQ_Router#
```

- A. HQ_Router last received an update from 190.171.23.12 at 3:30 am.
- B. If HQ_Router does not receive an update from 190.171.23.12 in 30 seconds, all routes from that source will be removed from the routing table.
- C. If HQ_Router does not receive an update from 190.171.23.12 in 30 seconds, all routes from that source will be flagged with a hold-down timer.
- D. 190.171.23.12 is expected to send an update to HQ_Router for network 190.172.0.0 in 3 minutes and 30 seconds.

10. Refer to the exhibit. Explain how the routes in the table are being affected by the status change on interface Ethernet0.

```

GW_Router# debug ip rip
RIP protocol debugging is on

<output omitted>

*Mar 1 00:19:36.804: %LINK-5-CHANGED: Interface Ethernet0, changed state to down
*Mar 1 00:19:36.805: RIP: sending v2 flash update to 224.0.0.9 via Ethernet1
(190.172.32.11)
*Mar 1 00:19:36.805: RIP: build flash update entries
*Mar 1 00:19:36.809:      190.171.23.0/24 via 0.0.0.0, metric 16, tag 0
*Mar 1 00:19:36.813:      208.149.23.32/27 via 0.0.0.0, metric 16, tag 0
*Mar 1 00:19:36.813:      208.149.23.64/27 via 0.0.0.0, metric 16, tag 0
*Mar 1 00:19:36.817:      208.149.23.96/27 via 0.0.0.0, metric 16, tag 0
*Mar 1 00:19:36.821:      208.149.23.128/27 via 0.0.0.0, metric 16, tag 0
*Mar 1 00:19:37.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0,
changed state to down
*Mar 1 00:19:39.131: RIP: sending request on Ethernet0 to 224.0.0.9
<output omitted>

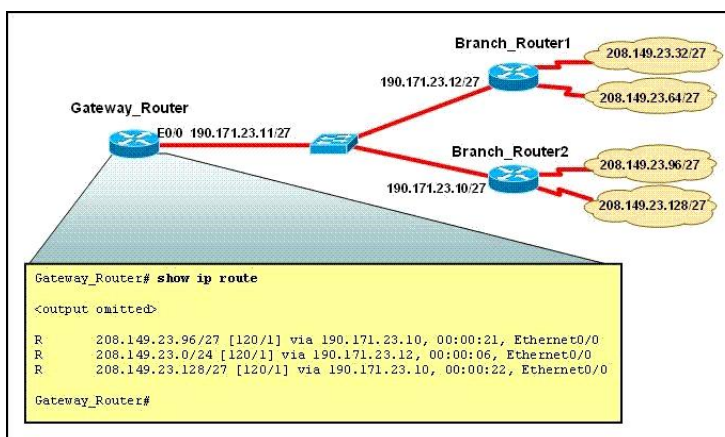
GW_Router#
  
```

- A. The router is requesting updates for these networks from routers that are connected to interface Ethernet1.
- B. The router is poisoning the routes and broadcasting the new path costs via interface Ethernet1.
- C. The router is receiving updates about unreachable networks from routers that are connected to interface Ethernet1.
- D. The router is poisoning the routes and multicasting the new path costs via interface Ethernet1.

11. Which three statements describe the differences between RIP version 1 and RIP version 2? (Choose three.)

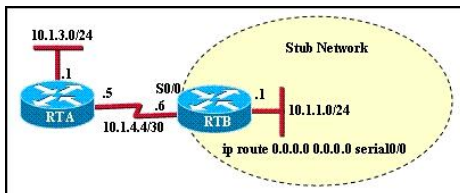
- A. RIP version 1 broadcasts updates whereas RIP version 2 uses multicasts.
- B. RIP version 1 multicasts updates while RIP version 2 uses broadcasts.
- C. Both RIP version 1 and RIP version 2 are classless routing protocols.
- D. RIP Version 2 is a classless routing protocol whereas RIP version 1 is a classful routing protocol.
- E. Both RIP version 1 and version 2 support authentication.
- F. RIP version 2 sends the subnet mask in updates and RIP version 1 does not.

12. Refer to the exhibit. What is the most likely reason for the disparity between the actual network numbers at the branches and the routes in the routing table on Gateway_Router?



- A. Gateway_Router is configured to receive only RIPv1 updates.
- B. Gateway_Router is configured to only receive RIPv2 updates.
- C. Branch_Router2 is configured to send both RIPv1 and RIPv2 updates.
- D. Branch_Router1 is configured to only send RIPv1 updates.

13. Refer to the exhibit. Subnet 10.1.3.0/24 is unknown to router RTB. Which router command will prevent router RTB from dropping a packet destined for the 10.1.3.0/24 network if a default route is configured?



- A. ip classless
- B. ip default-network
- C. network 10.1.1.0
- D. network 10.1.1.0 0.0.0.255 area 0

14. Refer to the output of the two show commands in the exhibit. If an administrator tries to ping host 10.1.8.5 from host 10.1.6.100, how will the ICMP packets be processed by Router A?

```
RouterA# show running-config
<some output text omitted>
router rip
 network 10.0.0.0
!
ip classless
RouterA# show ip route
<some output text omitted>
Gateway of last resort is 10.1.5.5 to network 0.0.0.0

10.0.0.0/24 is subnetted, 2 subnets
R   10.1.3.0 [120/1] via 10.1.2.2, 00:00:00, Serial0/0
C   10.1.2.0 is directly connected, Serial0/0
C   10.1.5.0 is directly connected, Serial0/1
C   10.1.6.0 is directly connected, FastEthernet0/0
R*  0.0.0.0/0 [120/1] via 10.1.5.5, 00:00:00, Serial0/1
```

- A. The packets will be discarded.
- B. The packets will be routed out the S0/0 interface.
- C. The packets will be routed out the S0/1 interface.
- D. The packets will be routed out the Fa0/0 interface.



6.7 真题解答***

1. 解: B

题目问: 参照图中的信息, 在 Router_1 上, 一条 RIP 的路由被标记为非法, 还要多长时间这条路由将被从路由表中删除? 本题考的是 RIP 定时器, 参照本章 6.1.3 节, 路由器上一条 RIP 从非法到被删除的时间间隔是 Flush 定时器减去 Invalid 定时器, 即 240-180=60 秒。

2. 解: CD

题目问: 图中的网络运行 RIPv2 协议, 网络已经收敛, 网络中的所有路由器工作都正

常。R1 路由器的 Fa0/0 接口 Down 了，网络中的路由器将使用哪两种方式响应这一改变？本题的考点是距离矢量路由协议的环路问题，可以参照第 5 章的 5.5.4 节。这涉及 RIP 关于环路避免的几种机制。A 选项说所有的路由器将参考拓扑数据库查找备份路由，RIP 协议没有拓扑表；B 选项说，路由器 R2 和 R3 标记 192.168.1.0 为不可达，并且在抑制定时器过期前，不接收 R1 发过来的其他路由更新，这里的抑制定时器只是针对 192.168.1.0，并不针对所有的路由条目；C 选项说因为水平分割，R2 将被阻止发送有关 192.168.1.0 的错误信息到 R1，这种说法是正确的；D 选项说当 R2 获知 R1 上 192.168.1.0 网络有一个无穷大度量值时，R2 将发送给 R1 到 192.168.1.0 网络有一个无穷大的度量值，这里说的是毒性反转（poison reverse），水平分割并不影响毒性反转；E 选项说 R1 将发送 LSA...，LSA 是链路状态通告，RIP 协议并不使用。综上所述，C 和 D 是正确答案。

3. 解：AC

题目问：根据给出的输出信息，下面哪种说法是正确的（选两个）？本题的难度相当大，考生使用排错法会更容易些。从 debug ip rip 命令的输出中，可以判断配置的是 RIPv1，因为使用的是广播更新（255.255.255.255），不是组播更新（224.0.0.9）；从 RtrA Fa0/0（172.16.1.1）发出的更新中，没有包括 172.16.0.0，可以得知 Fa0/0 接口启用了水平分割。同理，S0/0 接口也启用了水平分割，根据水平分割还可以得知 192.168.1.0 是从该接口学到的，因为发出的 192.168.1.0 网络有 2 跳，说明不是本路由器的直连路由，是从其他路由器学到，然后再发送出去的；还可以得知 192.168.168.0 是一个不可达的网络，因为有 16 跳；可以得知 RtrA 路由器 S0/0 接口的 IP 地址是 10.0.8.1，邻居路由器的 IP 地址是 10.0.15.2，并且这两个接口配置在同一个子网中，不然 debug 输出中会提示收到“ignored v1 update from bad source”，即忽略一个错误源的更新。根据前面的分析，A 选项说至少有两台路由器参与 RIP 进程是正确的；B 选项说 RtrA 路由器可以 ping 通 192.168.168.2 是错误的，因为 RtrA 可以得知 192.168.168.0 是一个不可达的网络；C 选项说 RtrA 可以 ping 通 10.0.15.2，通过前面的分析可以得知 10.0.15.2 是邻居路由器直连接口的 IP 地址，如果没有额外的限制（比如后面会介绍到 ACL，路由可以学到，并不能代表数据包可以到达并能成功返回）是可以 ping 通的，如果没有更好的选项，可以考虑该选项；D 选项说 RtrA 有三个接口参与 RIP 进程，从 debug 的输出中，可以看到 Fa0/0 向外发送两个路由条目，一个是学来的，另一个是本路由器 S0/0 直连接口的，S0/0 向外发送一个路由条目是本路由器 Fa0/0 直连接口的，并没有包含其他直连接口的路由，可以得知 RtrA 只有两个接口参与 RIP 进程。综上所述，A 和 C 是正确答案。如果是单选，则只能选 A。

4. 解：D

题目问：使用 VLSM 技术，分配一个 C 类的 IP 地址在点对点的串行线路上，什么样的子网掩码是高效的？在点到点的串行链路上只需要分配两个 IP 地址给两端就可以了，加上网络地址和广播地址，这个网段只需要 4 个 IP 地址，所以主机位只需要 2 位，那么网络位就有 30 位，对应的掩码是 255.255.255.252。

5. 解：BD

题目问：参照图，所有的路由器都被配置了“ip subnet-zero”（即允许使用全 0 和全 1 的 IP 子网），哪个网络地址将被配置在链路 A 和网络 A 上（选两个）？这是个 IP 地址规划的考题，Network A 中有 120 台主机，因此 Network A 中至少需要 122 个 IP 地址，根据公式 $2^n \geq 122$ ，可以解出 $n=7$ ，因此网络位为 $32-7=25$ ，容纳的 IP 地址为 128。因此 Network A

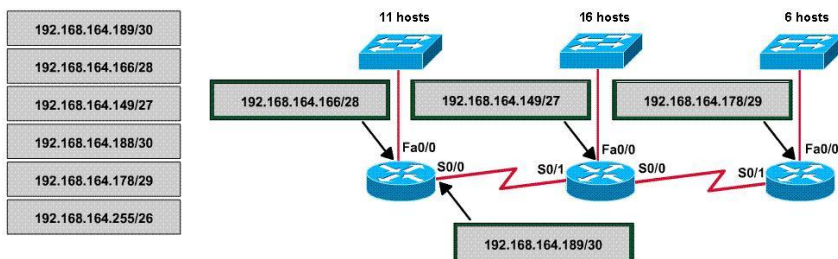
的网段就可以为 172.16.3.0/25 或 172.16.3.128/25。通过其他的设备分配的地址可以看到 172.16.3.0/25 的地址已经有一部分被分配出去了, 因此 Network A 分配的地址空间只能是 172.16.3.128/25。Link A 只需要有两个可用的 IP 地址, 因此网段中需要有 4 个地址, 根据公式 $2^n \geq 4$, 可以解出 $n=2$, 因此网络位为 $32-2=30$ 。而从其他路由器上的地址分配可以看到, 172.16.3.4~172.16.3.15、172.16.3.32~172.16.3.127 这些 IP 地址都已经分配出去了, 因此结合答案可以看到 Link A 的地址空间只能为 172.16.3.0/30。

6. 解: C

题目问: 根据图, 一个新的有 12 台主机的子网被添加到网络中, 哪一个子网地址可以提供足够的可用地址, 并且浪费尽量少的 IP 地址? 12 台主机, 主机位需要 4 位, 网络位则是 28 位, 因此 A 和 C 可以满足。又因为 192.168.10.80/28 中的 IP 地址包含在 192.168.10.64/27 中, 所以正确的答案只能是 C。

7. 解:

结果如下图所示:



这是一个拖拉题, 要求把左边的选项拖到右边对应的位置上, 左边有 6 个选项, 右边只有 4 个位置, 也就是会有多出的选项, 对多出的选项不用理会。题目中提到了可以使用全 0 和全 1 的子网(ip subnet-zero), 可以使用 VLSM(使用的路由协议是 RIPv2, 支持 VLSM)。要求以最节省 IP 地址的方式, 也就是要分配最合适的 IP 地址范围, 不要造成浪费。这里还有一点要提醒的是, 交换机上列出的主机数包括了路由器接口的 IP 地址。要提供 11 个可用的 IP 地址, 主机位需要 4 位, 网络位是 28 位; 同理, 要提供 16 个可用的 IP 地址, 网络位需要 27 位; 要提供 6 个可用的 IP 地址, 网络位需要 29 位; 要提供 2 个可用的 IP 地址, 网络位需要 30 位。该题中问的并不是网络地址, 而是路由器对应接口的 IP 地址, 要注意 IP 地址不是子网号或子网广播。

8. 解: ACE

题目问: 关于 RIPv2, 哪三个语句是正确的(选三个)? 首先要了解 RIPv2 是一个无类的路由协议, 在发送路由更新的时候是携带掩码的。它的 metric 的计算方式和 RIPv1 的相同, 仍然是根据跳数, 都是 16 跳即认为不可达。RIPv2 和 RIPv1 默认的管理距离都是 120。RIPv1 是以广播的形式发送更新, RIPv2 中采用的组播更新, 地址为 224.0.0.9。RIPv2 是支持认证的, 而在 RIPv1 中是没有这个功能的。RIPv2 是可以关闭自动汇总的, 而在 RIPv1 中是不能关闭的。

9. 解: B

题目问: 参照图中的输出, 关于从 190.171.23.12 学到的路由, 可以得出什么? 从输出

的 Last Update 00:03:30 可以得知, HQ_Router 路由器最后从 190.171.23.12 收到更新, 距离现在已经有 210 秒了, 从前面的输出中, 可以看到路由的非法时间和抑制时间都是 180 秒, 删除时间是 240 秒, 当前从 190.171.23.12 学到的路由都超过 180 秒没有更新, 再过 $240-210=30$ 秒将被从路由表中删除。

10. 解: D

题目问: 解释路由表中的路由怎样受 Ethernet0 端口状态变化的影响? 从输出中可以看到, 当 Ethernet0 状态 down 掉后, 路由器 GW_Router 把一些路由的跳数设成 16 跳, 并从 Ethernet1 接口以组播的方式向外发送更新, 使用的是距离矢量路由协议避免路由环路的一种方法——路由中毒 (route poisoning), 可以参照 5.5.4 节。综上所述, 路由器使用的是路由中毒, 并以组播方式从 Ethernet1 接口发送新的路径花费, D 选项正确。

11. 解: ADF

题目问: 哪三个语句描述了 RIPv1 和 RIPv2 的不同? 可以参照本章 6.4.2 节, A 选项说 RIPv1 是广播更新, 而 RIPv2 是组播更新, 正确; B 选项的说法与 A 相反, 则错误; C 选项说 RIPv1 和 RIPv2 都是无类路由协议, 错误, RIPv1 是有类路由协议, RIPv2 是无类路由协议; D 选项正确; E 选项说 RIPv1 和 RIPv2 都支持认证, 错误, RIPv1 不支持认证, RIPv2 支持认证; F 选项说 RIPv2 在更新中发送子网掩码, RIPv1 不发送子网掩码, 该说法正确。

12. 解: D

题目问: 分支路由器上的路由与 Gateway_Router 路由器上的路由表不一致, 最可能是什么原因? Gateway_Router 从分支路由器 2 上学到了两条明细路由, 即 208.149.23.96/27 和 208.149.23.128/27, 可以得知分支路由器 2 配置的是 RIPv2, 并且关闭了自动汇总。Gateway_Router 从分支路由器 1 上学到了一条汇总的主类网络路由, 有两种可能: 一是分支路由器 1 配置的是 RIPv1, 在主类网络的边界自动产生汇总的路由; 二是分支路由器 1 配置的是 RIPv2, 但没有关闭自动汇总。综上所述, A 选项说 Gateway_Router 只接收 RIPv1 的更新是错误的, 因为它已经从分支路由器 2 收到了 RIPv2 的更新; B 选项说 Gateway_Router 只接收 RIPv2 的更新也显得太绝对了, 如果分支路由器配置的是 RIPv1, 则 Gateway_Router 还需接收 RIPv1 的更新; C 选项说分支路由器 2 被配置成发送 RIPv1 和 RIPv2 的更新也不一定, 分支路由器 2 完全可以只运行 RIPv2; D 选项说分支路由器 1 被配置成只发送 RIPv1 的更新, 则最有可能导致图中的不一致。

13. 解: A

题目问: RTB 上配置了默认路由, 什么样的路由命令可以阻止 RTB 丢弃去往 10.1.3.0/24 的数据包? 本题考的是路由器的有类和无类路由行为, 可以参照本章的 6.5.2 节。因为 RTB 上有直连的 10.1.1.0/24, 如果使用的是有类路由行为, RTB 将丢弃去往 10.1.3.0/24 的数据包, RTB 需要使用无类路由行为, 命令是 ip classless。

14. 解: C

题目问: 根据 show running-config 和 show ip route 命令的输出, 如果管理员试着从主机 10.1.6.100 ping 主机 10.1.8.5, RouterA 如何处理 ICMP 的数据包? 从输出中可以看到路由器使用的是无类路由行为 (ip classless), 也可以看到 10.1.8.5 的明细路由没有出现在路由表中, 但 10.1.8.5 的父路由 10.0.0.0 出现在路由表中, 在 Router A 的路由表中有一条 RIP 的默认路由。根据本章 6.5.2 节介绍的“路由查找过程”, 可以得知 RouterA 将从 S0/1 接口把 ICMP 报文发出。

第 7 章

EIGRP***

本章主要介绍 EIGRP 的特性、分组类型、表的种类、度量值计算、非等值带宽负载均衡、路由汇总等相关内容。



7.1 EIGRP 概述和基本配置***

EIGRP (Enhanced Interior Gateway Routing Protocol, 增强内部网关路由协议) 是一种高级距离矢量、无类的路由选择协议。EIGRP 是增强的 IGRP (Interior Gateway Routing Protocol, 内部网关路由协议), IGRP 和 EIGRP 都是思科私有的协议, 只能运行在思科路由器上。

7.1.1 EIGRP 特性***

思科公司开发 EIGRP 的主要目的是创建一个无类别的 IGRP。EIGRP 作为一个高级的距离矢量, 拥有其他一些距离矢量路由协议所不具有的功能。EIGRP 的特性包括:

- **复合度量值** (metric composed)。EIGRP 和 IGRP 一样, 也使用带宽 (bandwidth)、负载 (load)、延时 (delay)、可靠性 (reliability), 默认只使用带宽和延时。EIGRP 的度量值是 IGRP 的度量值乘以 256, 有更大的度量值范围。
- **快速收敛**。EIGRP 依赖于使用一种先进的路由选择算法 DUAL (Diffusing Update Algorithm, 弥散修正算法), 通过在拓扑表中保存可行性后继, 相当于是次优路由, 当可用的路由消失后, 次优路由马上进入路由表。
- **100%无环路**。这还是与 DUAL 算法有关。
- **配置简单**。EIGRP 的基本配置和 IGRP 的配置差不多, 也比较简单。
- **可靠的更新**。EIGRP 采用 RTP (Reliable Transport Protocol, 可靠传输协议), 并为每一个邻居都保存一个重传列表。
- **建立邻居关系** (Establishing Adjacencies)。运行 EIGRP 的路由器中有 3 张表, 除了路由表外, 还有邻居表和拓扑表 (Neighbor Tables and Topology Tables)。
- **支持多种网络协议**。EIGRP 最具吸引力的特性之一是它的模块化设计。通过 PDM (Protocol-Dependent Modules, 协议相关模块), EIGRP 支持多种网络层被路由协议, 比如 IP、IPX、AppleTalk 等。
- **支持 VLSM 和 CIDR**。
- **能关闭自动汇总, 支持手工汇总**。
- **使用组播更新取代了广播更新**。使用的组播地址是 224.0.0.10。

- **支持等价和不等价的负载均衡。**RIP 和 OSPF 都不支持不等价的负载均衡。
- **和 IGRP 相互兼容。**IGRP 和 EIGRP 相互兼容，这种兼容提供了与 IGRP 路由器之间的无缝互操作性。
- **增量式更新。**EIGRP 不像 RIP 协议发送整个路由表，EIGRP 仅发送变化的路由。
- **路由标记。**EIGRP 将它从 IGRP 或任何外部源学到的路由标记为“EX”（外部），因为这些路由不是起源于 EIGRP 路由，而是通过其他方式学到的。本章 7.3 节有外部路由的举例。

虽然 EIGRP 的行为很像链路状态路由协议，但它仍然是一个距离矢量路由协议，所以被称为高级的距离矢量路由协议。

7.1.2 EIGRP 包格式*

EIGRP 被设计成一个网络层协议，协议号是 88，EIGRP 使用 RTP（Reliable Transport Protocol，可靠传输协议）传送和接收 EIGRP 的分组。

1. RTP

RTP 是一种传输层协议，它可以保证 EIGRP 分组有序地发送到所有的邻居。在 TCP/IP 网络中，主机使用 TCP 来保证传输的可靠性。EIGRP 是协议无关的，除了支持 IP 协议外，还要支持 IPX、AppleTalk 等协议，EIGRP 使用 RTP 作为专有的传输层协议来保证路由选择信息的发送，而不像 RIP 使用 UDP 协议的 520 端口。

虽然说 RTP 称为可靠传输协议，但也包括了可靠和不可靠的部分。有些数据分组需要被确认，则是可靠的；有些数据分组不需要被确认，可以认为是不可靠的。有关哪些分组是可靠的，哪些分组是不可靠的，在 7.1.3 节“EIGRP 分组类型”中会介绍到。

2. EIGRP 包格式

EIGRP 包格式如图 7-1-1 所示。

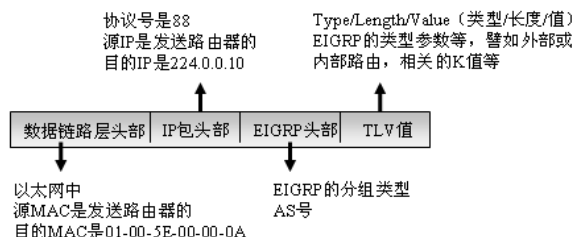


图 7-1-1 EIGRP 包格式

包括：

- **数据链路层头部：**EIGRP 使用的组播 IP 地址是 224.0.0.10，每个组播 IP 地址都有对应的 MAC 地址，组播 MAC 地址的厂商编码部分固定为“01-00-5E”，编号部分从具体的组播 IP 地址计算而来。这里不再介绍计算方法，224.0.0.10 对应的 MAC 地址是“01-00-5E-00-00-0A”。
- **IP 包头：**协议号是 88，源 IP 地址是发送路由器的 IP 地址，目的 IP 地址是 224.0.0.10。
- **EIGRP 头部：**EIGRP 和 IGRP 一样，也是内部网关协议，EIGRP 也需要配置 AS 号，在同一个 AS 内的路由器可以相互交换路由。EIGRP 依赖于几种不同的分组来维护

它的各种表，以及与邻居路由器的关系，分组类型包括：Hello（问候）、ACK（Acknowledgment，确认）、Update（更新）、Query（查询）、Reply（回复）。稍后介绍每种分组包的作用。

- **TLV 值：**包括类型/长度/值等。类型指的是 EIGRP 的外部路由还是内部路由，RIP 是没有办法区分是来自内部还是外部的，比如把静态路由重分布进 RIP 路由，在路由表中看到的都是“R”的标记。EIGRP 可以区分来自外部的路由，在路由表中显示为“D EX”，如果是内部的路由则显示为“D”。长度是指网络的前缀长度；值是目标网络。TLV 中还包括 EIGRP 的度量值计算权重，也就是相关的 K 值，在默认情况下，EIGRP 只使用带宽和延时。

7.1.3 EIGRP 分组类型**

EIGRP 使用 5 种分组类型来维护它的各种表，以及与邻居路由器的关系，分组类型包括：

1. Hello 分组

EIGRP 使用 Hello 分组来发现、验证和重新发现邻居路由器。EIGRP 以固定的时间间隔发送 Hello 分组，默认的 Hello 间隔与接口的带宽和类型有关。除小于或等于 1.544Mb/s 的多点帧中继链路是 60 秒外，其他链路都是 5 秒。

Hello 分组使用组播地址 224.0.0.10 发送。在邻居表中包含一个“保持时间”字段，记录了最后收到分组的时间。如果 EIGRP 路由器在保持时间间隔（hold time interval）内没有收到邻居路由器的任何 Hello 分组，就认为这个邻居出现了故障，邻居关系将会被重置。在默认情况下，保持时间是 Hello 间隔的 3 倍。

注意：EIGRP 仅在接口的主 IP 地址上发送 Hello 分组，在一个接口配置多个 IP 地址的情况下，如果两台相邻路由器接口的主 IP 地址没有宣告进 EIGRP，即使重地址宣告进 EIGRP，也建立不了邻接关系，更不可能交互路由。

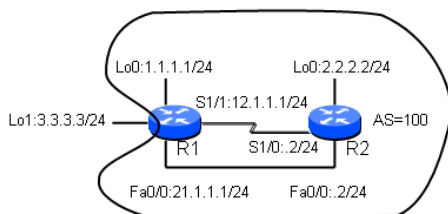


图 7-1-2 EIGRP 拓扑

为了大家能更好地理解相关分组，这里使用 EIGRP 配置图 7-1-2 中的网络。本章很多知识点的讲解都围绕这个实验，读者可以把配置文件保存起来，以便下次继续阅读本书，可以节约基本的配置时间。

有关 EIGRP 配置部分的语句附有详细解释。

R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#no cdp run
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int fa 0/0
R1(config-if)#ip add 21.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config-if)#int lo1
R1(config-if)#ip add 3.3.3.3 255.255.255.0
```

```
R1(config-if)#router eigrp 100
```

启用EIGRP路由选择协议进程，EIGRP和IGRP一样，都要使用AS号，这里的100就是AS号。AS标识了唯一的自治系统编号，它标识了属于一个互连网络中的所有路由器。为了保证不同的路由器之间可以相互学习路由，同一个AS内的不同路由器要使用相同的AS号。这一点与RIP不同，在RIP协议配置中，不需要使用AS号。

```
R1(config-router)#network 12.1.1.0 0.0.0.255
```

这里的12.1.1.0是网络号，0.0.0.255是反掩码，思科文档称为wildcard mask，翻译成中文是通配符掩码，这种叫法是不准确的，更准确的叫法是inverse of a subnet mask（反向子网掩码，简称反掩码）。网络号和反掩码一起决定了路由器的哪个接口参与EIGRP，以及路由器向哪个网络通告。如果省略反掩码，这里将自动使用主类网络号。假如路由器有两个接口，一个接口的IP地址是172.16.1.1/24，另一个接口的IP地址是172.16.2.1/24，其中172.16.2.1的接口并不运行EIGRP协议，这里就不能简单地写成network 172.16.0.0，而要写成172.16.1.0 0.0.0.255，这样的网络宣告中就不包括172.16.2.0/24的网络，172.16.2.1的接口不参与EIGRP进程。在如图7-1-2所示的拓扑中，这里可以写成network 12.0.0.0。这是除了可以使用主类网络号和子网号外，还可以使用超网，比如路由器有两个接口，一个接口的IP地址是172.16.1.1/16，另一个接口的IP地址是172.17.1.1/16，则可以简单地用一条network 172.0.0.0 0.255.255.255命令来宣告两个主类网络。如果路由器的所有接口都运行EIGRP，则可以简单地写成network 0.0.0.0，路由器R2使用的就是这条命令。路由器R1上没有使用network 0.0.0.0的原因是R1有一个接口并没有运行EIGRP，那就是Loopback 1。

```
R1(config-router)#network 21.1.1.0 0.0.0.255
```

```
R1(config-router)#network 1.1.1.0 0.0.0.255
```

R2的配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#no cdp run
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int fa 0/0
R2(config-if)#ip add 21.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int lo0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
R2(config-if)#router eigrp 100
R2(config-router)#network 0.0.0.0
```

使用下面的命令查看路由器R1 S1/1接口发送Hello分组的时间间隔。

```
R1#show ip eigrp interfaces detail s1/1
IP-EIGRP interfaces for process 100
```

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Se1/1	1	0/0	1035	0/15	6447	0

Hello interval is 5 sec
Next xmit serial <none>
Un/reliable mcasts: 0/0 Un/reliable ucasts: 4/12
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 3
Retransmissions sent: 1 Out-of-sequence rcvd: 2
Authentication mode is not set
Use unicast

从上面的输出中可以看到，R1的S1/1接口发送Hello分组的间隔是5秒。有的读者可能会问，前面提到了在小于或等于1.544Mb/s的多点帧中继链路上，默认的Hello间隔是60秒，这里为何是5秒？原因很简单，这里是点对点的链路，不是多点的帧中继链路。可以使用下面的命令修改Hello分组间隔。

```
R1(config)#int s1/1
R1(config-if)#ip hello-interval eigrp ?
<1-65535> Autonomous system number

R1(config-if)#ip hello-interval eigrp 100 ?
<1-65535> Seconds between hello transmissions
```

```
R1(config-if)#ip hello-interval eigrp 100 30
```

把 R1 S1/1 接口在 AS 100 中的 EIGRP Hello 分组的时间间隔设成 30 秒,这时会出现什么问题呢?读者会在 R2 上看到这样的提示信息:

```
R2#
*Jun 27 19:34:49.401: %DUAL-5-NBRCHANGE: IP-EIGRP (0) 100: Neighbor 12.1.1.1 (Serial1/0)
is down: holding time expired
*Jun 27 19:34:54.245: %DUAL-5-NBRCHANGE: IP-EIGRP (0) 100: Neighbor 12.1.1.1 (Serial1/0)
is up: new adjacency
```

R2 上提示与邻居 R1 的邻居关系 down 掉,稍后又提示与邻居 R1 建立了新的邻居关系,这种 down 和 up 的提示信息不断地重复出现。出现这种现象是因为修改 Hello 分组发送的间隔时间,保持时间间隔并不会自动更改为 Hello 间隔的 3 倍。结果是 R1 每隔 30 秒给 R2 发送一个 Hello 分组,而 R2 在 15 秒内收不到 R1 的 Hello 分组就认为邻居关系消失,解决的办法是修改保持时间。命令如下:

```
R2(config-if)#ip hold-time eigrp 100 90
```

把保持时间改成 90 秒,是 Hello 分组间隔的 3 倍。在路由器 R1 上使用“show ip eigrp neighbor”命令,查看 R1 的 EIGRP 邻居,显示如下:

```
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address          Interface      Hold Uptime    SRTT   RTO  Q  Seq
                               (sec)          (ms)        Cnt  Num
1  12.1.1.1           Se1/0         80 00:01:34     8    200  0  76
0  21.1.1.1           Fa0/0         12 03:36:29    16    200  0  17
```

从上面的输出中可以看到,R2 与 R1 分别使用串行接口和快速以太网接口建立了两次邻居关系,串行接口显示的可以保持时间是 80 秒,在正常情况下,该值不会小于 60 秒;快速以太网接口显示的保持时间是 12 秒,在正常情况下,该值不会小于 10 秒。

注意: 在 EIGRP 中,邻居路由器并不需要有相同的 Hello 间隔和保持时间。而在后面要讲到的 OSPF 协议中,邻居路由器必须有相同的 Hello 间隔和保持时间,否则邻居关系失败。

2. ACK (确认) 分组

EIGRP 路由器在交互期间,使用确认分组来表示收到了 EIGRP 分组,感觉有点像 TCP 的确认重传。EIGRP 接收路由器必须确认发送者的消息,保证在路由器间提供可靠的通信。与多播的 Hello 分组不同,确认分组是单播的,只发往特定的路由器。为了提高效率,确认分组也可以搭载在其他类型的 EIGRP 分组上,如回复分组。

3. Update (更新) 分组

当路由器发现新的邻居时,便使用更新分组。一台 EIGRP 路由器向新的邻居发送单播的更新分组使之可以被加入到拓扑表中。

当路由器检测到拓扑变化时也使用更新分组。在这种情况下,EIGRP 路由器向所有邻居发送组播的更新分组,提醒这一变化。

不管是单播还是组播的更新分组,都需要被确认,都是可靠传输的。

4. Query (查询) 分组

当 EIGRP 路由器需要从一个或所有的邻居那里得到指定的信息时,使用查询分组。如

果一台 EIGRP 路由器丢失了某条路由的后继，并且找不到可行性后继时，DUAL 算法则将这条路由置为活动状态。然后，路由器向所有邻居组播查询，寻找到达目的网络的后继。

查询分组可以是组播或单播发送，查询分组是可靠的，即需要被确认。

5. Reply（回复）分组

对邻居路由器的查询信息进行回复。回复分组总是单播发送的，并且是可靠的，即需要进行确认。

这 5 种分组类型有的以组播方式发送，有的以单播方式发送；有的是可靠的，有的是不可靠的，表 7-1-1 对它们进行了对比。

表 7-1-1 EIGRP 分组对照表

	Hello	ACK	Update	Query	Reply
组播还是单播	组播	单播	组播或单播	组播或单播	单播
是否可靠，即是否需要进行确认	不可靠	不可靠	可靠	可靠	可靠

7.1.4 EIGRP 表***

EIGRP 路由器在内存中保存邻居和可用的路由及拓扑信息，以便对变化做出快速反应。EIGRP 中有 3 张表：邻居表、路由表、拓扑表。

1. 邻居表（Neighbor Table）

邻居表是 EIGRP 中最重要的表，每台 EIGRP 路由器维护一个毗邻路由器的列表。EIGRP 对于所支持的每种被路由协议都有一个邻居表，比如 IP、IPX 和 AppleTalk 各有一张邻居表。

（1）邻居发现和恢复。运行简单距离矢量路由协议的路由器不与相邻路由器建立邻居关系，如 RIP 和 IGRP 路由器仅在配置的接口上广播更新，而 EIGRP 路由器需要与相邻的路由器建立邻接关系（adjacencies）才能交互路由信息。EIGRP 路由器通过互发 Hello 分组来建立邻接关系，两台相邻路由器要建立起邻接关系需要满足两个条件：

- 具有相同的 AS 号；
- 具有匹配的 K 值。

EIGRP 虽然是距离矢量路由协议，但和链路状态路由协议一样，需要使用 Hello 消息来建立邻接关系。由于 EIGRP 和链路状态路由协议一样，不会定时发送路由更新数据，因此，需要一些机制来帮助路由器认识到有新的路由器加入，或老的路由器离开。为了维持这一邻接关系，EIGRP 必须持续地从它们的邻居那里接收 Hello 消息。

隶属于不同 AS 的 EIGRP 路由器不会建立邻接关系，更不会共享路由信息。启用 EIGRP 路由进程时，需要指定路由器所在的 AS 号。

EIGRP 可以使用带宽、延时、负载和可靠性的复合度量值（Composite Metric），在默认情况下，EIGRP 使用带宽和延时，这是通过 K 值来控制的。在路由器 R1 上，执行“show ip protocols”命令查看 R1 上运行的协议，显示如下：

```
R1#show ip protocols
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
```

```

EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 100
EIGRP NSF-aware route hold timer is 240s
Automatic network summarization is in effect
Automatic address summarization:
  21.0.0.0/8 for Serial1/1, Loopback0
    Summarizing with metric 28160
  12.0.0.0/8 for FastEthernet0/0, Loopback0
    Summarizing with metric 2169856
  1.0.0.0/8 for Serial1/1, FastEthernet0/0
    Summarizing with metric 128256
Maximum path: 4
Routing for Networks:
  1.1.1.0/24
  12.1.1.0/24
  21.1.1.0/24
Routing Information Sources:
  Gateway         Distance      Last Update
  (this router)    90            00:03:41
  12.1.1.2         90            00:03:41
  21.1.1.2         90            00:03:41
Distance: internal 90 external 170

```

从上面的输出中，可以看到 EIGRP 的度量值权重是 $K1=1$ 和 $K3=1$ ， $K1$ 相当于是带宽， $K3$ 相当于是延时。可以使用“Router(config-router)#metric weights tos k1 k2 k3 k4 k5”命令来修改 K 值。ToS (Type of Services, 服务类型) 被用于 QoS (Quality of Services, 服务质量)，区分服务的等级，QoS 将在 CCNP 部分学到，这里仅支持 ToS=0。

比如，使用下面的命令取消延时，而仅使用带宽作为度量值。

```

R1(config)#router eigrp 100
R1(config-router)#metric weights 0 1 0 0 0 0

```

相邻的路由器如果 K 值不匹配，路由器会显示“*%DUAL-5-NBRCHANGE: IP-EIGRP (0) 100: Neighbor 12.1.1.2 (Serial1/1) is down: K-value mismatch”提示信息，从中可以看到两端的 K 值不匹配。

从上面的输出中还可看到，EIGRP 路由器所在的 AS 号是 100；EIGRP 默认使用的跳数是 100，而 RIP 仅支持到 15 跳；使用了自动汇总；默认支持 4 条路径进行负载均衡，最大可以支持到 16 条路径进行负载均衡，使用“R1(config-router)#maximum-paths 16”命令进行修改；运行 EIGRP 的网络，从中可以看出 Loopback 0 所在的网络 3.3.3.0/24 并没有运行 EIGRP；内部 EIGRP 的管理距离是 90，外部 EIGRP 的管理距离是 170，有关内部和外部管理距离，稍后进行演示。

图 7-1-3 演示了 EIGRP 建立邻接关系和交换路由信息的过程。

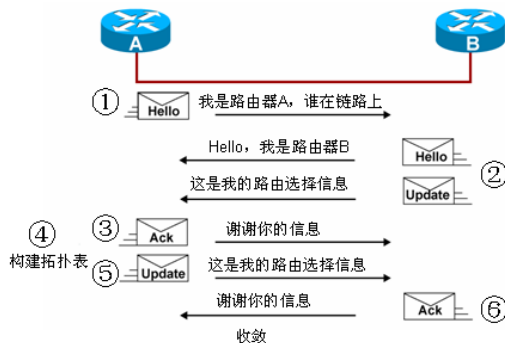


图 7-1-3 EIGRP 邻居相互交换路由信息

(2) 查看邻居表。在路由器 R1 上查看邻居表，显示如下：

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                Interface      Hold Uptime    SRTT   RTO  Q  Seq
                               (sec)          (ms)        Cnt Num
1   12.1.1.2                Se1/1         12 00:00:11    48   288  0  25
0   21.1.1.2                Fa0/0         11 00:28:46    24   200  0  23
```

显示的各项信息解释如下：

- “H”：列出邻居路由器被学到的顺序，0 是最早学到的。
- “Address”：邻居路由器接口的 IP 地址。
- “Interface”：路由器的本地接口。
- “Hold”：当前的保持时间，这是一个递减的数据值，但当有一个 Hello 包收到时，这个值重设成最大保持时间，如果这个值减小到 0，邻接关系 down 掉。
- “Uptime”：邻居路由器进入邻居表的时间。
- “SRTT”和“RTO”：SRTT(Smooth Round Trip Timer, 平均往返时间)和 RTO(Retransmit Interval, 重传间隔)将在 CCNP 部分讨论。
- “Q”：Q (Queue Count, 队列数) 一般总是为 0，如果大于 0，说明有 EIGRP 的包在排队，等待被发送。这也将 CCNP 部分讨论。
- “Seq”：Seq (Sequence Number, 序列号) 被用来追踪更新，查询和回复分组。这也将 CCNP 部分讨论。

passive-interface

如果在 EIGRP 的邻居表中，看不到应该有的邻居，除了查看链路接口的 IP 地址分配外，还要查看两端 EIGRP 的 AS 号是否匹配。特别值得一提的是 passive-interface (被动接口)，在 RIP 部分，介绍了可以把某个端配置成被动接口，来阻止该接口向外发送路由信息，但不影响接收路由信息。能否把两台相邻的 EIGRP 路由器一端的接口设置成被动接口，来阻止该路由器把路由宣告出去，同时不影响学习另一台路由器的路由呢？这是办不到的，EIGRP 不同于 RIP，只是从接口把路由广播出去，EIGRP 需要先互相发送 Hello 分组来建立邻接关系，如果把接口设成被动接口，该接口将不会向外发送 Hello 分组，不发送 Hello 分组，两台路由器就建立不起邻接关系，相互之间也不会交互路由。

2. 路由表

在路由器 R1 上使用 “show ip route” 命令，查看 R1 的路由表，显示如下：

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       1.1.1.0/24 is directly connected, Loopback0
D       1.0.0.0/8 is a summary, 00:02:41, Null0
D       2.0.0.0/8 [90/156160] via 21.1.1.2, 00:02:41, FastEthernet0/0
       3.0.0.0/24 is subnetted, 1 subnets
```



```

C    3.3.3.0 is directly connected, Loopback1
    21.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    21.1.1.0/24 is directly connected, FastEthernet0/0
D    21.0.0.0/8 is a summary, 00:02:41, Null0
    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.1.0/24 is directly connected, Serial1/1
D    12.0.0.0/8 is a summary, 00:02:44, Null0

```

这里看到的路由表与 RIP 中的路由表有很大差异，最明显的就是路由表中的条目比想象中的要多几条。路由表中第一行“1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks”是一条父路由，不是最终的路由，声明 1.0.0.0/8 使用了变长子网掩码，有 2 个子网，使用了两种子网掩码。第二行“C 1.1.1.0/24 is directly connected, Loopback0”是一条直连路由。第三行“D 1.0.0.0/8 is a summary, 00:02:41, Null0”是一条自动汇总产生的路由，EIGRP 和 RIP 在默认情况下都启用了自动汇总，路由协议会在网络边界自动汇总，但 RIP 不会在路由器本地产生一条自动汇总的路由，而 EIGRP 会在路由器本地产生一条自动汇总的路由，外出接口指向“Null0”，也是空接口，发往空接口的包将被丢弃。EIGRP 对路由汇总产生指向空接口的路由可以有效地避免路由环路。

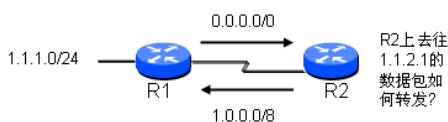


图 7-1-4 空接口汇总路由的优势

请看图 7-1-4 中的拓扑，如果运行的是 RIP 协议，采用的是无类路由行为（ip classless），R1 上配置了默认路由指向 R2，R1 上的 RIP 进程将网络 1.1.1.0/24 汇总成 1.0.0.0/8 宣告给 R2，R2 上如果有一个去往 1.1.2.1 的数据包，R2 将把数据包转发给 R1，R1 上没有 1.1.2.1 的明细路由，因为 R1 采用的是无类路由行为，R1 会把去往 1.1.2.1 的数据包根据默认路由，转发给 R2，然后 R2 再转发给 R1，路由环路形成。而如果运行的是 EIGRP 协议，R2 把数据包转发给 R1，R1 查询本地的路由表，可以知道除默认路由外，还有一条指向空接口的 1.0.0.0/8 路由可以匹配 1.1.2.1，根据选路原则的第一条，最长匹配优先，去往 1.1.2.1 的数据包将被发往空接口，也就是丢弃，不会产生路由环路。通过这里的讲解，相信读者已经明白了 EIGRP 自动产生指向空接口的汇总路由的好处。

接下来看 R1 路由表的第四行“D 2.0.0.0/8 [90/156160] via 21.1.1.2, 00:02:41, FastEthernet0/0”，这里的“D”表示该路由是通过 EIGRP 协议学习来的；“2.0.0.0/8”是 R2 发送过来的汇总路由；“[90/156160]”表示这条路由的管理距离是 90，度量值是 156160，EIGRP 的管理距离是 90（稍后介绍度量值的计算）；“via 21.1.1.2”表示 R1 去往 2.0.0.0/8 的下一跳是 21.1.1.2；“00:02:41”是这条路由存在的时间；“FastEthernet0/0”是本路由器的外出接口。从这条路由表中可以看出 R1 去往 2.0.0.0/8 的路由从快速的以太网链路走，而不像 RIP 只是简单地根据跳数进行负载均衡。

3. 拓扑表

拓扑表是由协议相关模块生成的。EIGRP 使用 DUAL 算法，根据邻居表和拓扑表提供的信息计算到每个目的地的最低成本路由。通过跟踪这些信息，EIGRP 路由器可以很快地确定并切换到替代路由。

EIGRP 路由器为每一种配置的被路由协议（如 IP、IPX 等）维护一个拓扑表。这个表包括路由器学到的所有目的地的路由条目，所学到的到某个目的地的所有路由都维护在拓扑表中。在路由器 R1 上使用“show ip eigrp topology”命令查看 R1 的拓扑表，显示如下：

```

R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(3.3.3.3)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 1.0.0.0/8, 1 successors, FD is 128256
    via Summary (128256/0), Null0
P 1.1.1.0/24, 1 successors, FD is 128256
    via Connected, Loopback0
P 2.0.0.0/8, 1 successors, FD is 156160
    via 21.1.1.2 (156160/128256), FastEthernet0/0
    via 12.1.1.2 (2297856/128256), Serial1/1
P 12.0.0.0/8, 1 successors, FD is 2169856
    via Summary (2169856/0), Null0
P 12.1.1.0/24, 1 successors, FD is 2169856
    via Connected, Serial1/1
P 21.0.0.0/8, 1 successors, FD is 28160
    via Summary (28160/0), Null0
P 21.1.1.0/24, 1 successors, FD is 28160
    via Connected, FastEthernet0/0

```

拓扑表中包括下列字段：

- **路由状态**：“P”表示路由是被动的（passive），即路由是稳定的和可用的；“A”表示路由是活动的（active），即路由正在使用 DUAL 重新计算的过程中，此时该条路由是不可用的。
- **目标网络**：2.0.0.0/8 就是一个目标网络。
- **后继（Successor）**：到远程网络的主要路由，对任何特定的路由可以有多达 4 条后继路由，它们可以有相等的或不相等的距离。如果使用的是不相等的后继，就是 EIGRP 非等值的负载均衡，这将在 EIGRP 的高级配置中演示。R1 去往 2.0.0.0/8 显示的是“1 successors”，即只有一条最佳路径。
- **FD（Feasible Distance，可行距离）**：这是一个到达远程网络的最佳路径，该路径的度量值最小，它将会出现在路由表中。可行距离是下一跳路由器的报告距离和本路由到下一跳路由器的距离之和。R1 去往 2.0.0.0/8 的路径有两条，距离分别是 2297856 和 156160，最小的距离 156160 成为可行距离，即从快速以太网接口到达 R2，然后再到达目的地。
- **路由来源**：是指最初发布这条路由的路由器的标识号。这一字段仅当路由是从其他的 EIGRP 路由器学到时才填入，如 2.0.0.0/8 是通过 12.1.1.2（via 12.1.1.2）或 21.1.1.2（via 21.1.1.2）学来的。
- **RD（Reported Distance，报告距离）**：是邻接路由器报告的到一个指定目标网络的距离。R1 去往 2.0.0.0/8 的路径有两条，一条是通过串行接口到达 R2，然后再到达目的地；另一条是通过快速以太网接口到达 R2，然后再到达目的地。不管从哪条路走，R2 的报告距离都是 128256，再加上 R2 不同接口的度量值，最后得出了从不同路径的可行距离，最小的可行距离将进入路由表。
- **接口信息**：通过本路由器的哪一个接口可以到达目标网络。

7.1.5 EIGRP 度量值计算**

EIGRP 使用复合的度量值（composite metric）计算到目标网络的最优路径。复合度量值可以是带宽、延时、可靠性和负载的组合，虽然说 MTU（Maximum Transmission Unit，

最大传输单元)也包含在路由更新中,但不被用来计算 IGRP 和 EIGRP 的度量值。

在 $K1$ 、 $K2$ 、 $K3$ 、 $K4$ 、 $K5$ 都不为 0 的情况下, EIGRP 度量值的计算公式是:

$$\text{Metric} = [K1 * \text{Bandwidth} + (K2 * \text{Bandwidth}) / (256 - \text{load}) + K3 * \text{Delay}] * [K5 / (\text{reliability} + K4)]$$

在默认情况下, $K1$ 和 $K3$ 等于 1, $K2$ 、 $K4$ 和 $K5$ 等于 0。EIGRP 度量值的计算公式简化成 $\text{Metric} = \text{Bandwidth} + \text{Delay}$ 。前面介绍过可以使用命令 “Router(config-router)#metric weights tos k1 k2 k3 k4 k5” 来调整各个度量值所占的比重。 $K1$ 影响的是带宽, $K2$ 影响的是负载, $K3$ 影响的是延时, $K4$ 和 $K5$ 影响的是可靠性。

$$\text{Metric} = (10000M / \text{源和目标之间的最低链路带宽} + \text{源和目标之间所有的链路延时总和} / 10) * 256$$

计算 EIGRP 度量值时,一定要清楚,所谓的带宽,是源和目标之间最低链路的带宽;所谓的延时,是源和目标之间所有链路的延时总和,单位是微秒,然后再除以 10。

这里来计算一下路由器 R1 到 R2 上 Loopback 0 接口所在网络的度量值,在 R2 上使用 “show interface loopback 0” 命令,部分显示如下:

```
R2#show interfaces loopback 0
Loopback0 is up, line protocol is up
Hardware is Loopback
Internet address is 2.2.2.2/24
MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
reliability 255/255, txload 1/255, rxload 1/255
```

从上面的输出中,可以看到 Loopback 0 接口的带宽是 8000Mb/s,延时是 5000μs。在 R1 上继续使用 “show int fa 0/0” 命令,部分显示如下:

```
R1#show int fa 0/0
FastEthernet0/0 is up, line protocol is up
Hardware is AmdFE, address is cc07.0ad4.0000 (bia cc07.0ad4.0000)
Internet address is 21.1.1.1/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
```

从上面的输出中,可以看到 Fa0/0 接口的带宽是 100Mb/s,延时是 100μs。在 R1 上继续使用 “show int s1/1” 命令,部分显示如下:

```
R1#show int s1/1
Serial1/1 is up, line protocol is up
Hardware is M4T
Internet address is 12.1.1.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
```

R1 到 2.0.0.0/8 的路径有两条,度量值计算如下:

$$\text{Fa0/0: Metric} = [10000/100 + (5000 + 100)/10] * 256 = 156160$$

$$\text{S1/1: Metric} = [10000/1.544 + (5000 + 20000)/10] * 256 \approx 2297856$$

在没有采用非等值带宽的情况下,最好的度量值将进入路由表,在 R1 上使用 “show ip route” 命令,可以验证 R1 到 2.0.0.0/8 的度量值确实是 156160。次好的路由不会进入路由表,可以使用 “show ip eigrp topology” 命令查看 R1 从串行接口到达 2.0.0.0/8 的距离,部分显示如下:

```
R1#show ip eigrp topology
P 2.0.0.0/8, 1 successors, FD is 156160
  via 21.1.1.2 (156160/128256), FastEthernet0/0
  via 12.1.1.2 (2297856/128256), Serial1/1
```

读者也可以使用 `shutdown` 命令关闭两台路由器间的快速以太网链路来验证使用串行接口的度量值。

在上面的命令中为何是查看 R1 的 Fa0/0 和 S1/1 接口，而不是查看 R2 的 Fa0/0 和 S1/0 接口呢？接下来使用一个小实验来说明这个问题。使用下面的命令来修改 R1 Fa0/0 接口的带宽：

```
R1(config)#int fa 0/0
R1(config-if)#bandwidth 1000000 这里的带宽值以 K 为单位，把带宽改成 1000Mb/s。
```

使用下面的命令来修改 R2 Fa0/0 接口的带宽：

```
R2(config)#int fa 0/0
R2(config-if)#bandwidth 10000000 这里把带宽改成 10000Mb/s。
```

！ 注意：上面使用 `bandwidth` 修改接口的带宽，仅仅会影响到计算，并不会影响实际的接口带宽。实际中建议使用 `delay` 修改延时来影响度量值，因为路由器中还有其他方面需要使用到带宽参数，比如 OSPF 也会使用到带宽。

此时，R1 到 2.0.0.0/8 的度量值是：

$$\text{Metric}=[10000/1000+(5000+100)/10]*256=133120$$

还是：

$$\text{Metric}=[10000/10000+(5000+100)/10]*256=130816$$

在路由器 R1 上进行验证，显示如下：

```
R1#show ip route eigrp | include 2.0.0.0/8
D    2.0.0.0/8 [90/133120] via 21.1.1.2, 00:00:39, FastEthernet0/0
    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D    12.0.0.0/8 is a summary, 00:50:21, Null0
```

“`show ip route eigrp | include 2.0.0.0/8`”这条命令是一个使用了过滤字符的 `show` 命令，“`show ip route`”用于查看整个路由表，“`show ip route eigrp`”仅查看 `eigrp` 的路由表；“`|`”是过滤符；“`include 2.0.0.0/8`”仅显示包含 2.0.0.0/8 的行。结果是过滤出 R1 上包含 2.0.0.0/8 的 EIGRP 路由。从上面的输出中可以看到，R1 去往 2.0.0.0/8 的度量值是 133120。从中可以得出结论，可以通过修改路由前进方向（路由前进方向与数据包的流向是相反的）上路由器进入接口的参数来修改度量值，也就是修改从 R2 到 R1 方向上进入接口（也就是 R1 的 Fa0/0 接口），而不是外出接口（R2 的 Fa0/0），来影响度量值。但在实际工作中，一般两端的参数都要修改，不然会影响返回的数据流量，造成往返数据流的不对称性。

在计算 EIGRP 度量值时，“`show ip eigrp topology`”命令可以显示某一条路由在本路由器上可行距离；总共有几条路径，每条路径的报告距离和最终距离，整个链路上的最小带宽是多少，整个链路的延时总和是多少等。在 R1 上查看 2.0.0.0 路由的拓扑数据库，显示如下：

```
R1#show ip eigrp topology 2.0.0.0
IP-EIGRP (AS 100): Topology entry for 2.0.0.0/8
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 133120
  Routing Descriptor Blocks:
    21.1.1.2 (FastEthernet0/0), from 21.1.1.2, Send flag is 0x0
      Composite metric is (133120/128256), Route is Internal
      Vector metric:
        Minimum bandwidth is 1000000 Kbit
        Total delay is 5100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```

```

12.1.1.2 (Serial1/1), from 12.1.1.2, Send flag is 0x0
Composite metric is (2297856/128256), Route is Internal
Vector metric:
  Minimum bandwidth is 1544 Kbit
  Total delay is 25000 microseconds
  Reliability is 255/255
  Load is 1/255
  Minimum MTU is 1500
  Hop count is 1

```



7.2 DUAL 算法和 EIGRP 排错**

DUAL (Diffusing Update Algorithm, 弥散修正算法) 是 EIGRP 使用的算法机制。本节讨论 DUAL 的相关术语和 DUAL 的工作方式。

7.2.1 DUAL 相关术语和 EIGRP 排错***

1. DUAL 相关术语

了解 DUAL 的相关术语相当重要，它们在 DUAL 的无环路 (loop-free) 机制中起到了核心的作用，这些术语包括：Successor、FD、RD 或 AD、FS 和 FC。其中 Successor、FD、RD 或 AD 在前一节都进行了介绍，接下来重点讨论一下 FS 和 FC。

- **Successor (后继)**：后继就是拥有到目标网络最少花费路由的路由器。

- **FD (Feasible Distance, 可行距离)**：到目标网络的最小度量值。

参照上一节的配置，从 R1 路由表中的 “D 2.0.0.0/8 [90/133120] via 21.1.1.2, 03:57:33, FastEthernet0/0”，可以得知 R1 去往 2.0.0.0/8 网络后继的 IP 地址是 21.1.1.2，可行距离是 133120。从 R1 的拓扑表中，也可以得知可行距离是 133120。R1 的拓扑表显示如下：

```

R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(3.3.3.3)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 1.0.0.0/8, 1 successors, FD is 128256
   via Summary (128256/0), Null0
P 1.1.1.0/24, 1 successors, FD is 128256
   via Connected, Loopback0
P 2.0.0.0/8, 1 successors, FD is 133120
   via 21.1.1.2 (133120/128256), FastEthernet0/0
   via 12.1.1.2 (2297856/128256), Serial1/1
P 12.0.0.0/8, 1 successors, FD is 2169856
   via Summary (2169856/0), Null0
P 12.1.1.0/24, 1 successors, FD is 2169856
   via Connected, Serial1/1
P 21.0.0.0/8, 1 successors, FD is 5120
   via Summary (5120/0), Null0
P 21.1.1.0/24, 1 successors, FD is 5120
   via Connected, FastEthernet0/0

```

- **RD (Reported Distance, 报告距离) 或 AD (Advertised Distance, 通告距离)**：下一跳路由器通告的到相同目标网络的距离。RD 和 AD 只是两种不同叫法，都是指邻居路由器的报告距离。

- **FS (Feasible Successor, 可行后继)**：DUAL 能够快速收敛的一个原因就是它保存了到目标网络的备份路径，也称为 FS。当拓扑发生改变时，DUAL 不需要重新计算，

马上就可以找到替代路径。FS 也是一个邻居，拥有到相同目标网络的无环路径，并且满足可行条件。

- **FC (Feasibility Condition, 可行条件)**：一个邻居路由器要成为 FS，必须能满足 FC (可行条件)。FC (可行条件) 是 RD (报告距离) 必须要小于 FD (可行距离)，也就是邻居路由器到相同目标网络的最小距离要小于本路由器到相同目标网络的最小距离，这样邻居路由器才满足 FC 的条件。

R1 的拓扑表显示如下：

```
P 2.0.0.0/8, 1 successors, FD is 133120
  via 21.1.1.2 (133120/128256), FastEthernet0/0
  via 12.1.1.2 (2297856/128256), Serial1/1
```

去往 2.0.0.0/8 的 FD 是 133120，R2 通过串行口的 RD 是 128256，满足 FC，即 $RD < FD$ 。路由器 R2 是 R1 去往 2.0.0.0/8 的 Successor 和 FS，当 R1 和 R2 间的以太网链路断开时，DUAL 不需要重新计算，R1 去往 2.0.0.0/8 的路由马上切换到串行链路上。其实能出现在“show ip eigrp topology”显示的拓扑表中的非 FD 路径，都满足 FC，都是 FS。这也就是说在“show ip eigrp topology”显示中没有出现的邻居路由器不满足 FC，不能成为 FS。

2. EIGRP 排错

在如图 7-2-1 所示的拓扑中，配置 EIGRP，完成网络的互连。编写如图 7-2-2 所示的文本文件，然后把对应的配置粘贴到 R1、R2 和 R3 的控制台中，完成配置。读者可以直接打开光盘中的“配置\7\eigrp 排错.txt”文件进行粘贴，经验丰富的工程师通过这种配置方式，可以大大节约配置的时间。初学者可能会因为没有在线帮助而觉得不习惯，甚至会输错命令，多加练习，即可克服。尤其是初学者，在粘贴时一定要观察控制台提示，看有没有错误命令的提示。

在路由器 R1 的控制台中粘贴图 7-2-2 中 R1 对应的配置，显示如图 7-2-3 所示，可以看到所有命令都被正确执行，没有出现错误提示。类似地粘贴 R2 和 R3 的配置。

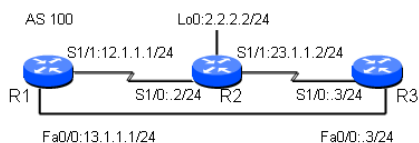


图 7-2-1 成为 FS 的条件



图 7-2-2 使用记事本编写配置文件

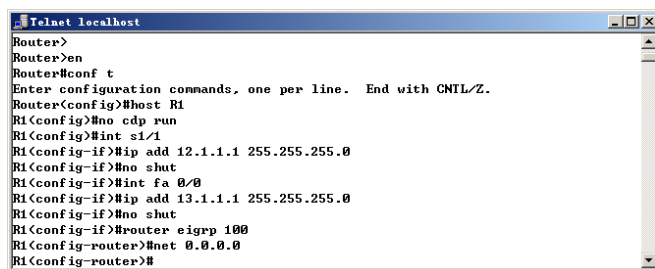


图 7-2-3 粘贴配置文件到路由器控制台

配置完成后，在 R1 上使用“show ip route”命令查看 R1 的路由表，显示如下：

```
R1#show ip route
D    2.0.0.0/8 [90/2297856] via 12.1.1.2, 00:02:52, Serial1/1
D    23.0.0.0/8 [90/2172416] via 13.1.1.3, 00:02:42, FastEthernet0/0
C    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.1.0/24 is directly connected, Serial1/1
D    12.0.0.0/8 is a summary, 00:03:09, Null0
C    13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    13.1.1.0/24 is directly connected, FastEthernet0/0
D    13.0.0.0/8 is a summary, 00:03:09, Null0
```

从上面的输出中可以看到，R1 去往 2.0.0.0/8 的后继只有一个，是路由器 R2，度量值是 2297856。如果 R1 到 R2 之间的串行链路断开，会发生什么情况呢？R1 有没有 FS 可用，需不需要重新执行 DUAL 算法来寻找到目标网络的最佳路由呢？在 R1 上使用“show ip eigrp topology”命令查看 R1 的拓扑表，显示如下：

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(13.1.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 2.0.0.0/8, 1 successors, FD is 2297856
   via 12.1.1.2 (2297856/128256), Serial1/1
P 12.0.0.0/8, 1 successors, FD is 2169856
   via Summary (2169856/0), Null0
P 12.1.1.0/24, 1 successors, FD is 2169856
   via Connected, Serial1/1
P 13.0.0.0/8, 1 successors, FD is 28160
   via Summary (28160/0), Null0
P 13.1.1.0/24, 1 successors, FD is 28160
   via Connected, FastEthernet0/0
P 23.0.0.0/8, 1 successors, FD is 2172416
   via 13.1.1.3 (2172416/2169856), FastEthernet0/0
   via 12.1.1.2 (2681856/2169856), Serial1/1
```

从上面的输出中可以看到，R1 去往 2.0.0.0/8 的 FD 是 2297856，在拓扑中只有一个下一跳地址，是后继，并没有 FS 可用。使用“show ip eigrp topology all-links”命令查看 R1 拓扑数据库中的所有内容，显示如下：

```
R1#show ip eigrp topology all-links
IP-EIGRP Topology Table for AS(100)/ID(13.1.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 2.0.0.0/8, 1 successors, FD is 2297856, serno 5
   via 12.1.1.2 (2297856/128256), Serial1/1
P 12.0.0.0/8, 1 successors, FD is 2169856, serno 4
   via Summary (2169856/0), Null0
```



```

P 12.1.1.0/24, 1 successors, FD is 2169856, serno 2
  via Connected, Serial1/1
P 13.0.0.0/8, 1 successors, FD is 28160, serno 3
  via Summary (28160/0), Null0
P 13.1.1.0/24, 1 successors, FD is 28160, serno 1
  via Connected, FastEthernet0/0
P 23.0.0.0/8, 1 successors, FD is 2172416, serno 7
  via 13.1.1.3 (2172416/2169856), FastEthernet0/0
  via 12.1.1.2 (2681856/2169856), Serial1/1

```

发现问题:

使用“show ip eigrp topology all-links”命令可以显示所有链路,即使下一跳路由器不满足 FC 的条件,不能成为 FS,也会在显示中出现。从上面的输出中,可以发现 R1 去往 2.0.0.0/8 的路径总共只有一条,和想象中的不一样, R1 有一条直接到达 R2 的路径,还有一条经过 R3 到达 R2 的路径,为何没有显示呢?在路由器 R3 上,使用“show ip route”命令查看路由表,显示如下:

```

R3#show ip route
D    2.0.0.0/8 [90/2300416] via 13.1.1.1, 00:15:02, FastEthernet0/0
    23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    23.1.1.0/24 is directly connected, Serial1/0
D    23.0.0.0/8 is a summary, 00:15:02, Null0
D    12.0.0.0/8 [90/2172416] via 13.1.1.1, 00:15:02, FastEthernet0/0
    13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    13.1.1.0/24 is directly connected, FastEthernet0/0
D    13.0.0.0/8 is a summary, 00:15:06, Null0

```

排错步骤 1:

R3 去往 R2 上 2.0.0.0/8 的路由竟然是从 R1 走的,这感觉非常不合理,根据对称性, R3 去往 R2 上的路由应该是直接发往 R2 才对。第一反应就是, R2 和 R3 之间的链路有问题,很可能是接口没有打开,在路由器 R2 和 R3 上使用“show ip int brief”命令,查看接口有没有被打开,显示如下:

```

R2#show ip int brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 unassigned      YES unset   administratively down down
Serial1/0      12.1.1.2       YES manual  up          up
Serial1/1      23.1.1.2       YES manual  up          up
Serial1/2      unassigned      YES unset   administratively down down
Serial1/3      unassigned      YES unset   administratively down down
FastEthernet2/0 unassigned      YES unset   administratively down down
Loopback0      2.2.2.2        YES manual  up          up

```

```

R3#show ip int brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 13.1.1.3       YES manual  up          up
Serial1/0      23.1.1.2       YES manual  up          up
Serial1/1      unassigned      YES unset   administratively down down
Serial1/2      unassigned      YES unset   administratively down down
Serial1/3      unassigned      YES unset   administratively down down
FastEthernet2/0 unassigned      YES unset   administratively down down

```

从上面的输出中可以看到, R2 和 R3 的所有应该打开的接口状态均正常,如果读者此时仔细查看,应该可以发现问题所在,即使你发现了问题所在,也请继续往下学习其他排错方法。如果没有人提醒,多数读者可能注意不到。我们这里先不指明,继续使用其他排错方法。

排错步骤 2:

从上面的输出中,基本可以排除物理层和数据链路层有故障。那接下来应该是网络层

了，测试 R2 和 R3 网络层的连接问题。有 50% 的读者可能会找出问题所在，假如你是那幸运的 50% 中的人，也请继续往下学习其他排错方法；假如你是那不幸的 50% 中的人，在路由器 R3 上 ping 路由器 R2 直连接口的 IP 地址 23.1.1.2，显示如下：

```
R3#ping 23.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/24/44 ms
```

从上面的输出中，发现网络层的连接也正常。

排错步骤 3:

再接下来应该是传输层的问题了，EIGRP 使用的 RTP 协议，对此几乎没有排错方法可用。现在应该查看 EIGRP 的路由表，因为 EIGRP 需要先建立邻居，然后才能交互路由。在 R2 或 R3 上使用“show ip eigrp neighbor”命令，查看 EIGRP 路由器的邻接关系。R3 上显示如下：

```
R3#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address          Interface      Hold Uptime    SRTT  RTO   Q    Seq
                               (sec)          (ms)          Cnt  Num
0   13.1.1.1          Fa0/0         13 00:41:33    17   200   0    14
```

从上面的输出中，可以发现 R2 和 R3 之间并没有建立邻接关系。这里回想一下，EIGRP 要建立邻接关系的两个条件：条件一，K 值匹配。很显然 K 值是匹配的，不然控制台会一直出现 K 值不匹配的提示，当然读者也可以使用“show ip protocols”命令进行验证。条件二，AS 号相同。既然 R3 可以和 R1 建立邻接，R3 与 R1 的 AS 号相同；R2 可以和 R1 建立邻接，R2 和 R1 的 AS 号相同，因此 R3 和 R2 的 AS 号也是相同的，当然读者也可以使用“show running-config”命令进行查看。

排错步骤 4:

既然建立邻接关系的条件都满足，为何还建立不起来邻接关系，会不会是因为没有收到对方发过来的 Hello 分组呢？在路由器 R2 和 R3 上分别使用“debug eigrp packets”命令，查看 EIGRP 包的发送情况。R3 的显示如下：

```
*Mar 1 01:16:44.923: EIGRP: Received HELLO on Serial1/0 nbr 23.1.1.2
*Mar 1 01:16:44.927: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0
*Mar 1 01:16:44.927: EIGRP: Packet from ourselves ignored
*Mar 1 01:16:46.847: EIGRP: Sending HELLO on Serial1/0
*Mar 1 01:16:46.851: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
*Mar 1 01:16:48.119: EIGRP: Sending HELLO on FastEthernet0/0
*Mar 1 01:16:48.123: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
*Mar 1 01:16:48.519: EIGRP: Received HELLO on FastEthernet0/0 nbr 13.1.1.1
```

从上面的输出中，可以发现 R3 从 R1 和 R2 收到了 Hello 分组。R2 的 debug 信息显示如下：

```
*Jun 28 21:45:42.859: EIGRP: Received HELLO on Serial1/0 nbr 12.1.1.1
*Jun 28 21:45:42.863: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ
un/rely 0/0
*Jun 28 21:45:45.563: EIGRP: Received HELLO on Loopback0 nbr 2.2.2.2
*Jun 28 21:45:45.563: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0
*Jun 28 21:45:45.563: EIGRP: Packet from ourselves ignored
*Jun 28 21:45:46.091: EIGRP: Received HELLO on Serial1/1 nbr 23.1.1.2
*Jun 28 21:45:46.091: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0
*Jun 28 21:45:46.091: EIGRP: Packet from ourselves ignored
```

从上面的输出中,可以发现 R2 从 R1 收到了 Hello 分组, R2 从环回接口收到了 Hello 分组(在 EIGRP 中,环回接口也会发送和接收 Hello 分组,可以使用 `passive-interface`,把环回接口设成被动接口,不影响网络的运行。但对物理接口不能使用被动接口,被动接口不发送 Hello 分组,EIGRP 邻接关系建立不起来,路由也无法交互了),R2 怎么还从 23.1.1.2 收到了 Hello 分组,难道 R3 s1/0 接口的 IP 地址也配成了 23.1.1.2,经查看,确实是 R3 的 S1/0 接口 IP 地址配错。

至此,原因找到。其实如果在排错步骤 1 中查看仔细,除了检查接口状态和协议状态外,多查看一下 IP 地址的分配,可能已经找到原因了。

排错步骤 2 中如果幸运地在 R2 上 ping 23.1.1.3,也能发现原因。从这里的排错也可以得到经验,以后 ping 测试时,双向都测试一下。

如果排错步骤 1、2 就解决了,也不需要排错步骤 3 和排错步骤 4 了。改正路由器 R3 的 S1/0 接口的 IP 地址,稍后 R3 的屏幕上会出现下面的提示:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 23.1.1.2 (Serial1/0) is up: new adjacency
```

提示 R3 已经与 R2 建立了邻接关系,在 EIGRP 中,默认使用了“`eigrp log-neighbor-changes`”命令,日志记录邻居的关系变化。如果使用加 `no` 的命令,关闭这个功能,就看不到邻居建立和断开的提示消息了。

如果重复的 IP 地址出现在以太网上,则比较容易发现错误。假设把路由器 R3 的 Fa0/0 接口的 IP 地址配成了 13.1.1.1,会在 R3 和 R1 的控制台中看到类似下面的报错信息:

```
*Mar 1 00:08:32.027: %IP-4-DUPADDR: Duplicate address 13.1.1.1 on FastEthernet0/0, sourced by cc07.02e0.0000
```

显示配置在 Fa0/0 接口的 IP 地址 13.1.1.1 重复,也就是 IP 地址冲突。另一个配置这个 IP 地址的设备的接口的 MAC 地址为“cc07.02e0.0000”。

再次在路由器 R1 上查看路由表、拓扑表,与之前显示的一样。再次使用“`show ip eigrp topology all-links`”命令查看 R1 拓扑表中的所有条目,与先前显示的有所不同,显示如下:

```
R1#show ip eigrp topology all-links
IP-EIGRP Topology Table for AS(100)/ID(13.1.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 2.0.0.0/8, 1 successors, FD is 2297856, serno 5
    via 12.1.1.2 (2297856/128256), Serial1/1
    via 13.1.1.3 (2300416/2297856), FastEthernet0/0
P 12.0.0.0/8, 1 successors, FD is 2169856, serno 4
    via Summary (2169856/0), Null0
P 12.1.1.0/24, 1 successors, FD is 2169856, serno 2
    via Connected, Serial1/1
P 13.0.0.0/8, 1 successors, FD is 28160, serno 3
    via Summary (28160/0), Null0
P 13.1.1.0/24, 1 successors, FD is 28160, serno 1
    via Connected, FastEthernet0/0
P 23.0.0.0/8, 1 successors, FD is 2172416, serno 13
    via 13.1.1.3 (2172416/2169856), FastEthernet0/0
    via 12.1.1.2 (2681856/2169856), Serial1/1
```

从上面的输出中,可以看到 R1 去往 2.0.0.0/8 的路径有两条,从 R2 走或从 R3 走。R2 是 Successor (后继); R3 不能成为 FS (可行后继)的原因是 RD (报告距离) 2297856 等于 FD (可行距离) 2297856,不满足 $RD < FD$ 的 FC (可行条件)。EIGRP 也正是使用可行条件的限制来阻止了路由的环路,一条从本路由器宣告出去的路由,通过其他路由器后,

再返回到本路由器时，该路由的报告距离一定大于可行距离，这样的路由不会成为后继，也不会成为可行后继。

为了节省配置时间，不要关闭路由器 R1、R2 和 R3，或者把配置拷贝出来，7.3 节的部分实验将在本实验的基础上完成。

7.2.2 DUAL 算法**

1. FSM (Finite State Machine, 有限状态机)

EIGRP 的核心部分是 DUAL 的有限状态机。有限状态机是一个抽象的机器，而不是一个机械装置与运动部件。FSM 定义一组可能的状态，如图 7-2-4 所示。

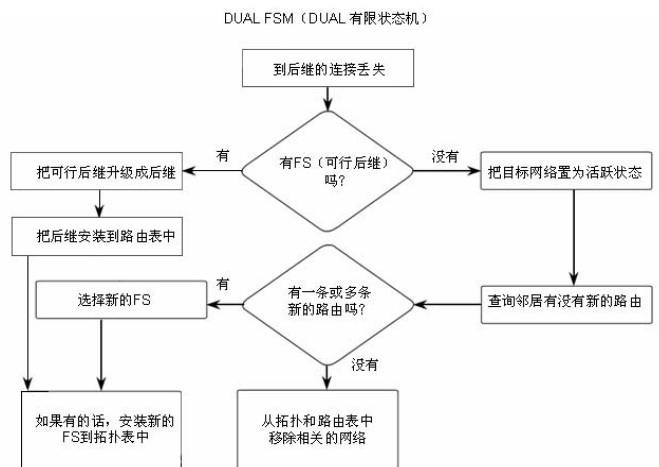


图 7-2-4 DUAL 有限状态机

可以使用“debug eigrp fsm”命令监视 EIGRP，比如在 R1 上打开 debug，然后关闭 S1/1 接口，再打开 S1/1 接口，debug 输出如下：

```

R1#debug eigrp fsm          打开监视 FSM。
EIGRP FSM Events/Actions debugging is on
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s1/1
R1(config-if)#shut
关闭 S1/1 接口，下面是 debug 信息的输出，这里有删减，仅显示了关于 2.0.0.0/8 的部分信息，CCNA 考试中不会涉及此内容。

*Mar 1 00:54:39.567: DUAL: Dest 12.0.0.0/8 entering active state.
*Mar 1 00:54:39.571: DUAL: Set reply-status table. Count is 1.
*Mar 1 00:54:39.571: DUAL: Not doing split horizon
*Mar 1 00:54:39.787: DUAL: rcvreply: 2.0.0.0/8 via 13.1.1.3 metric 2300416/2297856
*Mar 1 00:54:39.791: DUAL: reply count is 1
*Mar 1 00:54:39.791: DUAL: Clearing handle 1, count now 0
*Mar 1 00:54:39.795: DUAL: Freeing reply status table
*Mar 1 00:54:39.795: DUAL: Find FS for dest 2.0.0.0/8. FDis 4294967295, RDis 4294967295
found
*Mar 1 00:54:39.799: DUAL: Removing dest 2.0.0.0/8, nexthop 12.1.1.2, info source
12.1.1.2
*Mar 1 00:54:39.803: DUAL: RT installed 2.0.0.0/8 via 13.1.1.3
*Mar 1 00:54:39.807: DUAL: Send update about 2.0.0.0/8. Reason: metric chg
*Mar 1 00:54:39.811: DUAL: Send update about 2.0.0.0/8. Reason: new if
R1(config-if)#end
  
```

R1#un all *undebug all 的缩写, 关闭所有的 debug 命令。*
All possible debugging has been turned off

2. DUAL 算法示例

在图 7-2-5 中, 网络处于收敛状态。各路由器的拓扑数据库如图中右边部分所示。路由器 C 到达网络 10.1.1.0/24 的 FD (可行距离) 是 3, 后继是路由器 B, 可行后继是路由器 D。路由器 E 既不是后继也不是可行后继, 原因是 AD (通告距离是 3) 等于 FD (可行距离是 3), 不满足通告距离小于可行距离的可行条件。

路由器 D 到达网络 10.1.1.0/24 的 FD 是 2, 后继是路由器 B, 没有可行后继。路由器 C 不满足可行条件。路由器 E 的后继是路由器 D, 路由器 D 中没有路由器 E 的信息。

路由器 E 到达网络 10.1.1.0/24 的 FD 是 3, 后继是路由器 D, 没有可行后继。路由器 C 不满足可行条件。

网络拓扑发生变化, 路由器 B 和路由器 D 之间的链路断开, 如图 7-2-6 所示。路由器 D 将最先受到影响, 路由器 D 的后继路由器消失。

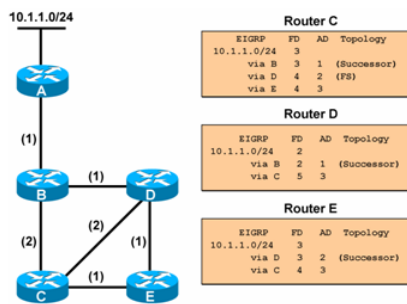


图 7-2-5 网络收敛

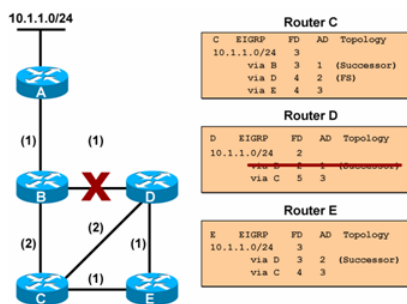


图 7-2-6 网络拓扑发生变化

如图 7-2-7 所示。因为路由器 D 没有 FS，路由器 D 向所有的邻居查询关于 10.1.1.0/24 的路由。此时路由器 D 上关于 10.1.1.0/24 的路由条目处于活跃状态，并等待邻居路由器 E 和 C 的回复。

路由器 C 收到路由器 D 的查询消息，路由器 C 从拓扑表中清除路由器 D 的信息。

路由器 E 收到后继路由器的查询，路由器 E 的后继消失。

如图 7-2-8 所示。路由器 C 收到路由器 D 的查询，路由器 C 把自己到达网络 10.1.1.0/24 的 FD 通告给路由器 D。路由器 D 收到路由器 C 的回复信息后，更新拓扑数据库。

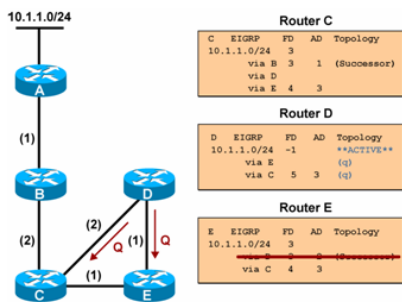


图 7-2-7 路由器 D 查询所有邻居

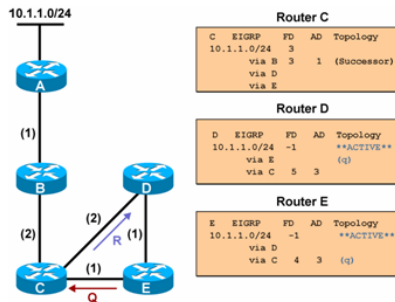


图 7-2-8 继续查询或回复

路由器 E 丢失了后继路由器，路由器向除后继外的所有邻居路由器查询，也就是向路由器 C 查询。路由器 E 处于活跃状态，等待路由器 C 的回复。

路由器 C 收到路由器 E 的查询后，更新拓扑表，清除路由器 E 的信息。

如图 7-2-9 所示。路由器 D 收到路由器 C 的回复，但还没有收到路由器 E 的回复，路由器 D 继续处于活跃状态，等待路由器 E 的回复。

路由器 E 收到路由器 C 的回复，路由器 E 更新自己的拓扑信息。路由器 E 到达网络 10.1.1.0/24 的 FD 是 4。

如图 7-2-10 所示。路由器 E 收到路由器 C 的回复，路由器 E 有到网络 10.1.1.0/24 的后继，路由器 E 处于被动状态。路由器 E 把自己的 FD 通告给 D。

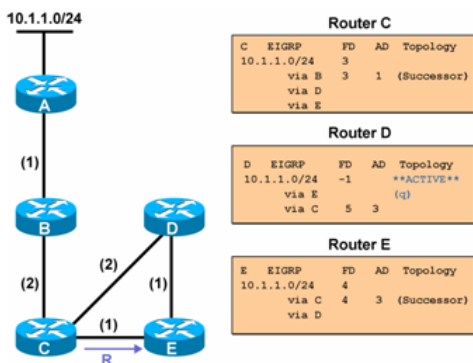


图 7-2-9 路由器 E 收到回复

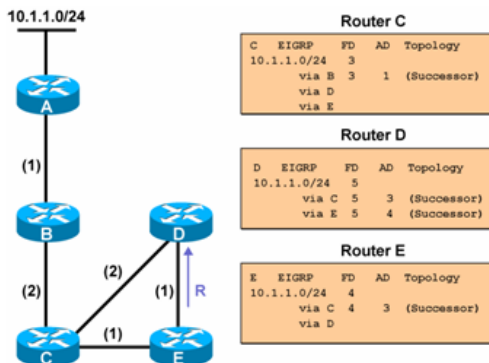


图 7-2-10 路由器 D 收到所有的回复

路由器 D 收到了路由器 E 的回复。路由器 D 收到了所有的回复，路由器 D 更新拓扑表，计算出到达网络 10.1.1.0/24 的 FD 是 5，有两条等值的路径。

如图 7-2-11 所示。网络中的所有路由器都处于被动状态，网络再次收敛。

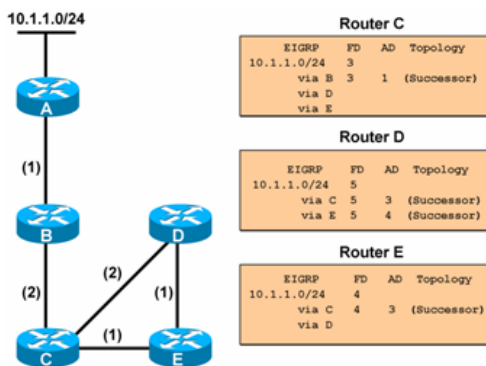


图 7-2-11 网络再次收敛

7.3 EIGRP 高级配置**

本节介绍 EIGRP 的高级配置，包括 EIGRP 的手工汇总、EIGRP 的非等值负载均衡、EIGRP 的验证、EIGRP 的外部路由、EIGRP 的带宽分配和调整。

7.3.1 EIGRP 非等值负载均衡

IGRP 和 EIGRP 可以支持非等值的负载均衡，而 RIP 和 OSPF 等协议则没有这个功能，

仅能支持等值的负载均衡。这里继续使用如图 7-2-1 所示的拓扑，继续使用如图 7-2-2 所示记事本中的配置，只是不要再把 R3 S1/0 接口的 IP 地址配错。

配置完成后，在 R1 上查看路由表，显示如下：

```
R1#show ip route
D    2.0.0.0/8 [90/2297856] via 12.1.1.2, 00:02:28, Serial1/1
D    23.0.0.0/8 [90/2172416] via 13.1.1.3, 00:02:28, FastEthernet0/0
    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.1.0/24 is directly connected, Serial1/1
D    12.0.0.0/8 is a summary, 00:02:51, Null0
    13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    13.1.1.0/24 is directly connected, FastEthernet0/0
D    13.0.0.0/8 is a summary, 00:02:52, Null0
```

R1 去往 23.0.0.0/8 的路径只有一条，如果运行的是 RIP 协议，这里将会出现两条等值的路径，因为 RIP 只是简单地根据跳数判断路由的优劣。而 EIGRP 使用的是复合度量值，默认与带宽和延时有关。在 R1 的路由表中为何是从 R3 去往 23.0.0.0/8，而不是从 R2 去往 23.0.0.0/8？有的读者可能会说 R1 和 R3 之间是 100Mb/s 链路，比 R1 和 R2 之间的 1.544Mb/s 链路要快，其实并不是因为链路带宽的原因，EIGRP 计算度量值时，使用的是链路上的最小带宽，R2 和 R3 之间也是 1.544Mb/s 的链路，不管是从 R2 还是从 R3，链路的最低带宽都是 1.544Mb/s。在路由器 R1 上查看 23.0.0.0 网络的拓扑可以找出原因，显示如下：

```
R1#show ip eigrp topology 23.0.0.0
IP-EIGRP (AS 100): Topology entry for 23.0.0.0/8
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2172416
Routing Descriptor Blocks:
 13.1.1.3 (FastEthernet0/0), from 13.1.1.3, Send flag is 0x0
   Composite metric is (2172416/2169856), Route is Internal
   Vector metric:
     Minimum bandwidth is 1544 Kbit
     Total delay is 20100 microseconds
     Reliability is 255/255
     Load is 1/255
     Minimum MTU is 1500
     Hop count is 1
 12.1.1.2 (Serial1/1), from 12.1.1.2, Send flag is 0x0
   Composite metric is (2681856/2169856), Route is Internal
   Vector metric:
     Minimum bandwidth is 1544 Kbit
     Total delay is 40000 microseconds
     Reliability is 255/255
     Load is 1/255
     Minimum MTU is 1500
     Hop count is 1
```

从上面的输出中，可以看到 R1 去往 23.0.0.0 的路径有两条，从 R2 或 R3 都可以到达。从 R2 走的度量值是 2681856，其中 R2 报告过来的距离是 2169856，从 R1 到目标网络的最低链路带宽是 1.544Mb/s，延时总和是 40000μs。从 R3 走的度量值是 2172416，其中 R3 报告过来的距离是 2169856，从 R1 到目标网络的最低链路带宽是 1.544Mb/s，延时总和是 20100μs。最小度量值的路径进入路由表，R3 成为 R1 去往 23.0.0.0/8 的后继路由器。从上面的显示中，可以看出 R1 选择 R3 作为后继的原因不是因为带宽，而是因为延时，以太网接口的延时默认是 100μs，串行接口的默认延时是 20000μs，可以在路由器 R1 上使用“show int fa 0/0”命令和“show int s1/1”命令进行查看。

用较大的度量值 2681856 除以较小的度量值 2172416， $2681856/2172416 \approx 1.2345$ ，取不小于 1.2345 的整数，也就是 2。使用 variance 命令配置不等价因子，配置命令如下：

```
R1(config)#router eigrp 100
```



```
R1(config-router)#variance 2
```

variance 值 n 是根据度量值计算出来的，用来分担网络的流量，这里计算出的值是 2，度量值小于 $FD \times 2$ 的路径有可能进入路由表，至于为什么说有可能，稍后会介绍到。variance 值为 n 的意义相当于快速链路发 n 个包，慢速链路发 1 个包。配置完成后，再次查看 R1 的路由表，显示如下：

```
R1#show ip route
D    2.0.0.0/8 [90/2297856] via 12.1.1.2, 00:07:38, Serial1/1
D    23.0.0.0/8 [90/2172416] via 13.1.1.3, 00:07:38, FastEthernet0/0
      [90/2681856] via 12.1.1.2, 00:07:38, Serial1/1
      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.1.0/24 is directly connected, Serial1/1
D    12.0.0.0/8 is a summary, 00:07:38, Null0
      13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    13.1.1.0/24 is directly connected, FastEthernet0/0
D    13.0.0.0/8 is a summary, 00:07:38, Null0
```

注意到 R1 去往 23.0.0.0/8 的路径有两条了。

前面提到满足度量值 $< n \times FD$ （这里的 n 是 variance 值，FD 是可行距离）的路径可能会进入路由表，为什么是可能呢？读者在 R1 上查看 2.0.0.0 网络的拓扑，显示如下：

```
R1#show ip eigrp topology 2.0.0.0
IP-EIGRP (AS 100): Topology entry for 2.0.0.0/8
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2297856
Routing Descriptor Blocks:
 12.1.1.2 (Serial1/1), from 12.1.1.2, Send flag is 0x0
   Composite metric is (2297856/128256), Route is Internal
   Vector metric:
     Minimum bandwidth is 1544 Kbit
     Total delay is 25000 microseconds
     Reliability is 255/255
     Load is 1/255
     Minimum MTU is 1500
     Hop count is 1
 13.1.1.3 (FastEthernet0/0), from 13.1.1.3, Send flag is 0x0
   Composite metric is (2300416/2297856), Route is Internal
   Vector metric:
     Minimum bandwidth is 1544 Kbit
     Total delay is 25100 microseconds
     Reliability is 255/255
     Load is 1/255
     Minimum MTU is 1500
     Hop count is 2
```

R1 经 R3 去往 2.0.0.0/8 的度量值是 2300416，小于 2 倍的 FD，即 $2300416 < 2 \times 2297856$ ，从前面 R1 的路由表中，却看不到去往 2.0.0.0/8 有两条路径，这是因为给 R3 的路径不满足可行条件，即报告距离要小于可行距离。从上面的输出中，可以看到 R3 的报告距离等于可行距离。所以说一条次好的路径要进入 EIGRP 路由表，除了要满足度量值 $< n \times FD$ 外，还要满足 $RD < FD$ 。

7.3.2 EIGRP 汇总***

1. 自动汇总

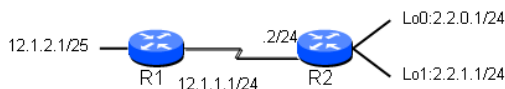


图 7-3-1 路由汇总

EIGRP 协议和 RIP 协议一样，默认自动在主类网络的边界汇总。在如图 7-3-1 所示的拓扑中，R1 和 R2 上各会有几条最终路由（路由条目中包括下一跳路由器 IP 地址或本路由

器外出接口的路由，也就是除父路由外的级别 1 和级别 2 的路由）呢？

路由器 R1 配置如下：

```
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ip add 12.1.2.1 255.255.255.128
R1(config-if)#router eigrp 100
R1(config-router)#net 12.1.1.0 0.0.0.255
R1(config-router)#net 12.1.2.0 0.0.0.127
```

路由器 R2 配置如下：

```
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int lo0
R2(config-if)#ip add 2.2.0.1 255.255.255.0
R2(config-if)#int lo1
R2(config-if)#ip add 2.2.1.1 255.255.255.0
R2(config-if)#router eigrp 100
R2(config-router)#net 0.0.0.0
```

配置完成后，在 R1 上查看路由表，显示如下：

```
R1#show ip route
D    2.0.0.0/8 [90/2297856] via 12.1.1.2, 00:04:24, Serial1/1
    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.1.0/24 is directly connected, Serial1/1
C    12.1.2.0/25 is directly connected, Loopback0
```

从上面的输出中可以看出，R1 上有 3 条最终路由，“D 2.0.0.0/8 [90/2297856]”是从 R2 学过来的汇总路由，还有两条是直连路由。读者此时可以思考一下 R2 会出现几条最终路由呢？在 R2 上查看路由表，显示如下：

```
R2#show ip route
    2.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    2.2.0.0/24 is directly connected, Loopback0
C    2.2.1.0/24 is directly connected, Loopback1
D    2.0.0.0/8 is a summary, 00:34:22, Null0
    12.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C    12.1.1.0/24 is directly connected, Serial1/0
D    12.0.0.0/8 is a summary, 00:00:03, Null0
D    12.1.2.0/25 [90/2297856] via 12.1.1.1, 00:02:11, Serial1/0
```

从上面的输出中可以看出，R2 上居然有 6 条最终路由，3 条直连路由是大家都能想到的。接下来分析 3 条 EIGRP 的路由：

第一条“D 2.0.0.0/8 is a summary, 00:34:22, Null0”，是 R2 上的一条汇总路由，EIGRP 默认使用的是“auto-summary”，当 R2 把 2.2.0.0/24 和 2.2.1.0/24 从 R2 的 S1/0 接口宣告出去时，S1/0 接口的 IP 地址是 12.1.1.2/24，这里已经是 2.0.0.0/8 网络的边界了，R2 自动对两条明细路由进行汇总，汇总成主类网络 2.0.0.0/8。EIGRP 和 RIP 不同，EIGRP 会自动在本地产生一条指向 Null 0 接口的汇总路由，至于为何要生成一条指向 Null 0 接口的汇总路由，前面已经解释过了，主要是用来避免路由环路。

第二条“D 12.0.0.0/8 is a summary, 00:00:03, Null0”，是 R2 上的另一条汇总路由，当 R2 把 12.1.1.0/24 和 12.1.2.0/24 从 R2 的 Lo0 和 Lo1 接口宣告出去时，Lo0 和 Lo1 接口的

IP 地址属于 2.0.0.0/8，这里已经是 12.0.0.0/8 网络的边界了，R2 自动对两条明细路由进行汇总，汇总成主类网络 12.0.0.0/8。有的读者不免要问，为何在 R1 上没有自动汇总呢？原因在于 R1 上的两个接口都处在 12.0.0.0/8 这个主类网络中，没有主类网络的边界，不会自动产生汇总。

特别值得一提的是，在 EIGRP 中不可以把物理接口设成被动接口，但可以把环回接口设成被动接口来减小资源的占用。使用下面的命令把 R2 的两个环回接口设成被动接口：

```
R2(config)#router eigrp 100
R2(config-router)#passive-interface default
R2(config-router)#no passive-interface s1/0
```

此时，再次在 R2 上查看路由表，显示如下：

```
R2#show ip route
 2.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    2.2.0.0/24 is directly connected, Loopback0
C    2.2.1.0/24 is directly connected, Loopback1
D    2.0.0.0/8 is a summary, 00:27:14, Null0
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.1.0/24 is directly connected, Serial1/0
D    12.1.2.0/25 [90/2297856] via 12.1.1.1, 00:07:32, Serial1/0
```

从上面的输出中不能再看到 12.0.0.0/8 的路由了，因为两个环回接口都不向外发送路由更新，12.1.1.0/24 和 12.1.2.0/24 都不会被自动汇总，没有自动汇总，也就不会产生一条指向 Null 0 接口的汇总路由了。

第三条“D 12.1.2.0/25 [90/2297856] via 12.1.1.1, 00:02:11, Serial1/0”，是 EIGRP 从 R1 学到的远程网络，从这里可以看出 EIGRP 是支持 VLSM 的。

2. 手工汇总

EIGRP 与 RIP 一样，如果在不连续子网的情况下，自动汇总可能会造成路由不可达的问题，解决的办法就是关闭自动汇总。关闭自动汇总的命令如下：

```
R2(config)#router eigrp 100
R2(config-router)#no auto-summary
```

此时查看 R2 的路由表，显示如下：

```
R2#show ip route
 2.0.0.0/24 is subnetted, 2 subnets
C    2.2.0.0 is directly connected, Loopback0
C    2.2.1.0 is directly connected, Loopback1
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.1.0/24 is directly connected, Serial1/0
D    12.1.2.0/25 [90/2297856] via 12.1.1.1, 00:08:30, Serial1/0
```

从上面的输出中可以看到，R2 取消自动汇总后，不再产生指向 Null 0 接口的汇总主类网络路由。查看 R1 的路由表，显示如下：

```
R1(config-router)#do show ip route
 2.0.0.0/24 is subnetted, 2 subnets
D    2.2.0.0 [90/2297856] via 12.1.1.2, 00:03:11, Serial1/1
D    2.2.1.0 [90/2297856] via 12.1.1.2, 00:03:11, Serial1/1
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.1.0/24 is directly connected, Serial1/1
C    12.1.2.0/25 is directly connected, Loopback0
```

从上面的输出中可以看到，R2 不再向 R1 发送汇总路由，改成了两个明细路由。过多的明细路由会占用路由器的内存空间，影响查找的速度，还可能带来网络的不稳定性。使用下面的命令，在路由器 R2 上进行手工汇总：

```
R2(config)#router eigrp 100
R2(config-router)#no auto-summary
R2(config-router)#exit
R2(config)#int s1/0
R2(config-if)#ip summary-address eigrp 100 2.2.0.0 255.255.254.0
```

这里的 100 是 AS 号，2.2.0.0 255.255.254.0 是网络号和对应的子网掩码。EIGRP 汇总路由的管理距离是 5，也可在该命令的最后手工指定一个管理距离。

在 R2 上手工汇总后，在 R2 上查看路由表，显示如下：

```
R2(config-router)#do show ip route
  2.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    2.2.0.0/24 is directly connected, Loopback0
D    2.2.0.0/23 is a summary, 00:15:37, Null0
C    2.2.1.0/24 is directly connected, Loopback1
  12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.1.0/24 is directly connected, Serial1/0
D    12.1.2.0/25 [90/2297856] via 12.1.1.1, 00:30:13, Serial1/0
```

再在 R1 上查看路由表，显示如下：

```
R1#show ip route
  2.0.0.0/23 is subnetted, 1 subnets
D    2.2.0.0 [90/2297856] via 12.1.1.2, 00:02:59, Serial1/1
  12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.1.0/24 is directly connected, Serial1/1
C    12.1.2.0/25 is directly connected, Loopback0
```

从上面的输出中可以看出，R2 上的手工汇总已经生效。从上面的演示中，读者要好好地领会关闭自动汇总采用手工汇总的用法和结果。比如关闭自动汇总会影响本路由器向外发送的路由，并不会影响其他路由器发往本路由器的路由。手工汇总也是在向外发送路由的路由器上进行汇总，并会在汇总路由器本地产生一条指向 Null 0 接口的汇总路由。

EIGRP 的自动汇总或手工汇总会影响到无类（ip classless）路由行为，因为汇总路由会产生指向 Null 0 接口的路由，路由器根据最长匹配原则，如果有更具体的路由，不会继续查找超网路由或默认路由，发往 Null 0 接口的数据包将会被丢弃。

不要关闭路由器 R1 和 R2，继续下面的配置。

7.3.3 EIGRP 外部路由*

接着上面的实验，在路由器 R1 上新增一个 Loopback 1，IP 地址是 1.1.1.1/24。在路由器 R2 上使用“show ip route”命令，发现不了 R1 上环回接口的路由，这是因为 R1 的 EIGRP 进程中并没有宣告 Lo1 所在的网络。

这里不使用路由宣告的方式，而是使用路由重发布（redistribute），把 R1 上直连接口的路由重发布进 EIGRP，R1 的配置如下：

```
R1(config)#router eigrp 100
R1(config-router)#redistribute connected
```

重发布直连路由，也就是把直连接口的路由重发布进 EIGRP 进程。有关重发布将在 CCNP 部分讨论。

R1 配置完成后，马上在路由器 R2 上查看路由表，显示如下：

```
R2#show ip route
  1.0.0.0/24 is subnetted, 1 subnets
D EX  1.1.1.0 [170/2297856] via 12.1.1.1, 00:04:34, Serial1/0
  2.0.0.0/24 is subnetted, 2 subnets
C    2.2.0.0 is directly connected, Loopback0
C    2.2.1.0 is directly connected, Loopback1
  12.0.0.0/24 is subnetted, 2 subnets
C    12.1.1.0 is directly connected, Serial1/0
D    12.1.2.0 [90/2297856] via 12.1.1.1, 00:18:31, Serial1/0
```

从上面的输出中，可以看到一条“D EX 1.1.1.0 [170/2297856] via 12.1.1.1, 00:04:34, Serial1/0”的路由，“D EX”表示这条路由是 EIGRP 的外部路由，不是起源 EIGRP 内部，比如通过重发布等方式进入 EIGRP 进程的。EIGRP 外部路由的默认管理距离是 170。从这里也可以看出 EIGRP 的快速收敛，如果是 RIP 协议，对网络拓扑的改变有时需要几分钟才能收敛。

可以在拓扑表中看到该路由的详细信息，R2 显示如下：

```
R2#show ip eigrp topology 1.1.1.0/24
IP-EIGRP (AS 100): Topology entry for 1.1.1.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2297856
  Routing Descriptor Blocks:
    12.1.1.1 (Serial1/0), from 12.1.1.1, Send flag is 0x0
      Composite metric is (2297856/128256), Route is External
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 12.1.2.1
        AS number of route is 0
        External protocol is Connected, external metric is 0
        Administrator tag is 0 (0x00000000)
```

从上面的输出中，可以看到 1.1.1.0/24 是外部路由，重发布的是直连路由，当然还可以重发布静态路由或其他动态路由协议。假设 R1 是企业边界路由器，R1 上有一条默认路由指向 ISP（Internet 服务提供商），可以在 R1 上使用重发布，把默认路由重发布进 EIGRP，使内部的 EIGRP 路由器可以学到这条默认路由。R1 配置如下：

```
R1(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2
R1(config)#router eigrp 100
R1(config-router)#redistribute static
```

这里只是在 R1 上添加一条默认路由，如果是在生产环境中，应该是指向 ISP 的路由器。

重发布静态路由，默认路由也是静态路由中的一种。

在路由器 R2 上查看路由表，显示如下：

```
R2#show ip route
  1.0.0.0/24 is subnetted, 1 subnets
D EX   1.1.1.0 [170/2297856] via 12.1.1.1, 00:12:58, Serial1/0
  2.0.0.0/24 is subnetted, 2 subnets
C       2.2.0.0 is directly connected, Loopback0
C       2.2.1.0 is directly connected, Loopback1
  12.0.0.0/24 is subnetted, 2 subnets
C       12.1.1.0 is directly connected, Serial1/0
D       12.1.2.0 [90/2297856] via 12.1.1.1, 00:26:56, Serial1/0
D*EX 0.0.0.0/0 [170/2297856] via 12.1.1.1, 00:00:10, Serial1/0
```

从上面的输出中，可以看到“D*EX 0.0.0.0/0”，这是从 EIGRP 外部学到的默认路由。如果在拓扑表中查看该路由的详细信息，可以发现这条路由起源于静态路由。此外，在 EIGRP 中还可以使用“ip default-network”命令来宣告默认路由，这一点与 RIP 协议相同。

7.3.4 EIGRP 验证*

EIGRP 和 RIPv2 一样，也支持验证，验证配置的方法也相似。在全局配置模式下创建密钥链，在接口模式下调用密钥链和指定验证方式。有关 EIGRP 验证的配置，CCNA 不做要求，这里仅给出配置。R1 的配置如下：

```
R1(config)#key chain test
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco
R1(config-keychain-key)#int s1/1
R1(config-if)#ip authentication key-chain eigrp 100 test
R1(config-if)#ip authentication mode eigrp 100 md5
```

R1 配置完成后,可以在 R1 的控制台上看到“%DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 12.1.1.2 (Seial1/1) is down: authentication mode changed”的提示信息,此时 R1 和 R2 之间的验证失败。在 R2 端也启用 EIGRP 验证,配置如下:

```
R2(config)#key chain test
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco
R2(config-keychain-key)#int s1/0
R2(config-if)#ip authentication key-chain eigrp 100 test
R2(config-if)#ip authentication mode eigrp 100 md5
```

配置完成后,邻居关系重新建立起来,路由也可正常学习。

7.3.5 EIGRP 性能调整*

在默认情况下,EIGRP 协议最多只使用一个接口 50%的带宽来传递 EIGRP 信息,这主要是为了防止 EIGRP 进程过度占用链路,导致正常通信没有足够的带宽。可以在接口下使用“ip bandwidth-percent eigrp”命令来调整 EIGRP 可以使用接口带宽的百分比。

假如一个接口的默认带宽是 1.544Mb/s(物理接口显示的速率),可实际支持的带宽只有 154kb/s(可能是做了速率限制)。EIGRP 协议默认要使用物理接口带宽的 50%,也就是 700kb/s,实际可用的带宽只有 154kb/s,这将导致正常通信带宽的不足,可以使用下面的命令更改 EIGRP 可以使用的带宽百分比:

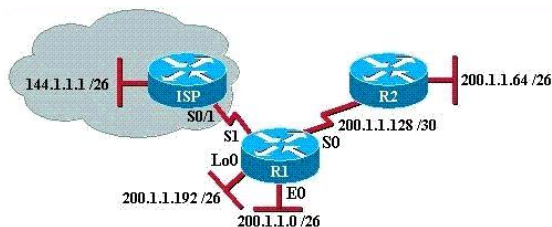
```
Router(config-if)#ip bandwidth-percent eigrp 100 5
```

这里的 100 是 EIGRP 路由器所在的 AS 号,5 是 EIGRP 协议占用接口带宽的百分比,即 5%,大概为 70kb/s。



7.4 真题精选***

- Which statements are true about EIGRP successor routes? (Choose two.)
 - A successor route is used by EIGRP to forward traffic to a destination.
 - Successor routes are saved in the topology table to be used if the primary route fails.
 - Successor routes are flagged as "active" in the routing table.
 - A successor route may be backed up by a feasible successor route.
 - Successor routes are stored in the neighbor table following the discovery process.
- Which tables of EIGRP route information are held in RAM and maintained through the use of hello and update packets? (Choose two.)
 - neighbor table
 - SPF table
 - RTP table
 - topology table
 - query table
 - DUAL table
- What can be determined from the router output shown in the graphic?



Gateway of last resort is 0.0.0.0 to network 0.0.0.0

```

200.1.1.0/24 is variably subnetted, 5 subnets, 3 masks
C    200.1.1.192/26 is directly connected, Loopback0
C    200.1.1.128/30 is directly connected, Serial0
D    200.1.1.64/26 [90/2195456] via 200.1.1.130, 00:02:15, Serial
D    200.1.1.0/24 is a summary, 00:00:41, Null0
C    200.1.1.0/26 is directly connected, Ethernet0
200.1.2.0/30 is subnetted, 1 subnets
C    200.1.2.4 is directly connected, Serial1
S*  0.0.0.0/0 is directly connected, Serial1

```

- A. 200.1.1.64 is a default route.
 - B. The output shows that there are three default routes.
 - C. The output came from router R2.
 - D. The output came from a router that has four physical interfaces.
 - E. EIGRP is in use in this network.
4. Refer to the exhibit. Why does RouterA show multiple unequal cost paths to network 192.168.81.0/24?

```

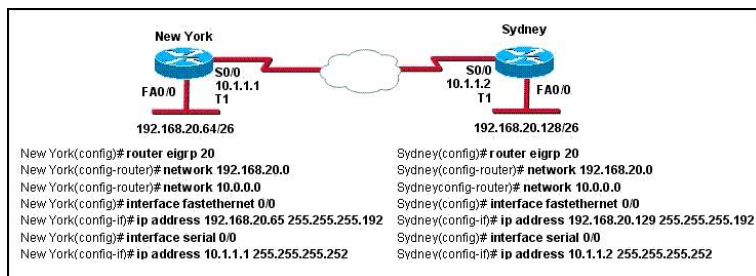
RouterA# show ip eigrp topology
IP-EIGRP Topology Table for AS(109)/ID(192.168.80.28)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

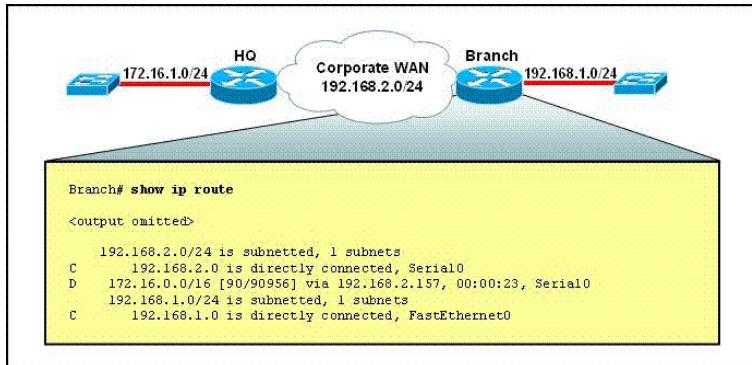
P 192.168.90.0/24 255.255.255.0, 2 successors, FD is 0
   via 192.168.80.28 (46251776/46226176), Ethernet0
   via 192.168.81.28 (46251776/46226176), Ethernet1
   via 192.168.80.31 (46277376/46251776), Serial0
P 192.168.81.0/24 255.255.255.0, 1 successors, FD is 307200
   via Connected, Ethernet1
   via 192.168.81.28 (307200/281600), Ethernet1
   via 192.168.80.28 (307200/281600), Ethernet0
   via 192.168.80.31 (332800/307200), Serial0

```

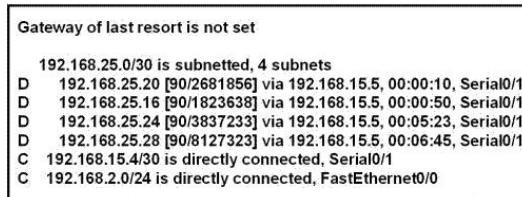
- A. A variance was configured for EIGRP autonomous system 109.
 - B. The EIGRP topology table displays all routes to a destination.
 - C. The EIGRP topology table shows only backup routes to a destination.
 - D. Multiple floating static routes were configured to network 192.168.81.0 via interface Serial0.
5. Which routing protocol by default uses bandwidth and delay as metrics?
- A. RIP
 - B. BGP
 - C. OSPF
 - D. EIGRP
6. Why has the network shown in the exhibit failed to converge?



- A. The no auto-summary command needs to be applied to the routers.
 - B. The network numbers have not been properly configured on the routers.
 - C. The subnet masks for the network numbers have not been properly configured.
 - D. The autonomous system number has not been properly configured.
 - E. The bandwidth values have not been properly configured on the serial interfaces.
7. Refer to the exhibit. The Branch router displays knowledge of a route to network 172.16.0.0/16. The actual network number at headquarters is 172.16.1.0/24. Why does the network number appear as it does in the routing table?

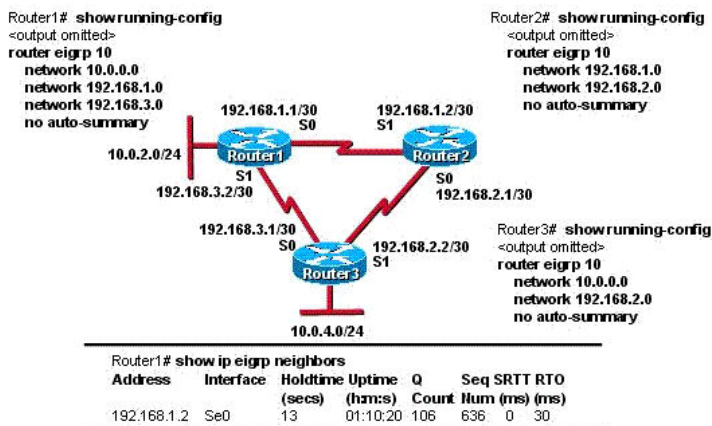


- A. The Branch router has a static route configured for the 172.16.0.0/16 network.
 - B. The routing protocol on the HQ router is using automatic route summarization.
 - C. The Branch router is configured to summarize to classful boundaries.
 - D. The routing protocol on the Branch router has been misconfigured.
 - E. The routing protocol that is forwarding this route only sends classful updates.
8. Refer to the exhibit. Which address and mask combination represents a summary of the routes learned by EIGRP?



- A. 192.168.25.0 255.255.255.240
 - B. 192.168.25.0 255.255.255.252
 - C. 192.168.25.16 255.255.255.240
 - D. 192.168.25.16 255.255.255.252
 - E. 192.168.25.28 255.255.255.240
 - F. 192.168.25.28 255.255.255.252
9. IP addresses and routing for the network are configured as shown in the exhibit. The network administrator issues the show ip eigrp neighbors command from Router1 and receives the output shown below the topology. Which statement is true?

- A. It is normal for Router1 to show one active neighbor at a time to prevent routing loops.
 B. Routing is not completely configured on Router3.
 C. The IP addresses are not configured properly on the Router1 and Router3 interfaces.
 D. The no auto-summary command configured on the routers prevents Router1 and Router2 from forming a neighbor relationship.



7.5 真题解答***

1. 解：AD

题目问：关于 EIGRP 的后继路由，哪些语句是正确的（选两个）？本题可以参考本章的 7.2.1 节，后继路径（Successor）是路由器选出的最优路径，将被放入路由表，路由器将选择这条路径到达目的地。而 Feasible successor 则是 Successor 的备份路径，不进入路由表，但记录在拓扑表中，如果 Successor 路径出了问题，就立即将 Feasible Successor 路径转为 Successor 路径，并被放入路由表。A 选项说后继路由被 EIGRP 用来转发流量到目的地，正确；B 选项说后继路由被保存在拓扑表中，如果首选路由失败，后继路由将被使用，这描述的是可行性后继路由的特征，错误；C 选项说后继路由在路由表中被标记为“活跃”状态，EIGRP 对于发出的查询，在没有收到应答前，将该路由标记为“活跃”状态，后继路由是稳定的路由，不会被标记为“活跃”状态，该选项错误；D 选项说后继路由可能被可行性后继路由备份，正确；E 选项说后继路由跟随发现过程被存储在邻居表中，该说法错误。

2. 解：AD

题目问：EIGRP 的哪一个表被保存在 RAM 中，并且依靠使用 hello 和 update 包来维护（选两个）？本章 7.1.4 节介绍了 EIGRP 中有 3 张表，即邻居表、拓扑表和路由表，EIGRP 依靠 hello 和 update 包维护邻居表和拓扑表。

3. 解：E

题目问：从图中路由器的输出，可以得出什么？因为在路由标记上有一个 D，表示这条路由是从 EIGRP 学到的，所以肯定是有 EIGRP 运行在网络中的。接下来仔细看输出中的直连路由：从 200.1.1.192/26 是直连 Loopback0 口，可以推断出这个信息是 R1 上的信息。D 200.1.1.0/24 is a summary, Null0: 表示这是一条汇总的 EIGRP 的路由。S* 0.0.0.0/0 is

directly connected, serial1: 表示这是一条默认的路由, 外出接口为 serial。综上所述, A 选项说 200.1.1.64 是默认路由, 路由前面的字母 D, 表示的是 EIGRP 学来的路由, 故 A 错; B 选项说有三条默认路由, 错误, 图中有两条 EIGRP 路由, 一条默认路由; C 选项说图中的输出来自 R2, 错误, 图中的输出来自 R1; D 选项说路由器有 4 个物理接口, 4 条直连路由中有一条来自环回接口, 路由器只有 3 个物理接口; E 选项说 EIGRP 在网络中被使用, 正确。

4. 解: B

题目问: 为何 RouterA 显示多条到 192.168.81.0/24 网络的不等花费? 本题可以参考本章 7.2.1 节, 图中显示的是拓扑表, EIGRP 的拓扑表中可以显示到目标的所有路径。经实验测试发现, “show ip eigrp topology” 命令只列出所有能满足可行性条件的路径, 也就是后继路径和可行性后继路径, “show ip eigrp topology all-links” 命令才能显示出所有的路径。读者可以在本章 7.2.1 节 EIGRP 排错完成后, 分别使用这两条命令验证这里的说法, 也有可能是路由器 IOS 版本的问题, 但针对本题来讲, 只有 B 是最适合的答案。

5. 解: D

题目问: 哪一种路由协议默认使用带宽和延时作为度量值? 在所学的路由协议中使用复合度量值的协议只有 IGRP 和 EIGRP, 而它们在默认的情况下都是使用带宽和延时来计算度量的。

6. 解: A

题目问: 为什么图中的网络会收敛失败? 注意图中的路由器 New York 上有 192.168.20.64/26 子网, 路由器 Sydney 上有 192.168.20.128/26 子网, 它们都属于主类网络 192.168.20.0/24, 如果不关闭自动汇总, 两台路由器上都会产生一条自动汇总的 EIGRP 路由 “D 192.168.20.0/24 is a summary, 00:14:35, Null0”, 两台路由器也会彼此向对方通告 192.168.20.0/24 的路由, 因为路由器本身已经有 192.168.20.0/24 指向 Null0 口的路由, 彼此都不学习对方的路由, 结果是彼此都学不到对方/26 的子网路由, 网络收敛失败。综上所述, 应该把 “no auto-summary” 命令应用在路由器上。

7. 解: B

题目问: Branch 路由器上显示了 172.16.0.0/16 的路由, 而在 HQ 路由器上实际的网络是 172.16.1.0/24, 为什么在 Branch 路由器上出现的路由表却是 172.16.0.0/16? 首先注意到这是一条标记为 “D” 的路由, 即是 EIGRP 学过来的路由, HQ 路由器上的 172.16.1.0/24 子网, 被自动汇总成有类网络 172.16.0.0/16, 这是因为没有关闭 EIGRP 自动汇总产生的现象。因为 HQ 路由器上没有关闭 EIGRP 自动汇总, 有些考生可能会错误地认为是 Branch 路由器上没有关闭自动汇总造成的, 实际上不是, HQ 路由器产生汇总后的路由 172.16.0.0/16 发送给 Branch 路由器, Branch 路由器将照单全收, 如果 HQ 路由器发送过来的路由是 172.16.1.0/24 子网路由, 而 Branch 路由器没有关闭自动汇总, Branch 路由器也不会对学过来的 172.16.1.0/24 子网路由进行汇总, 可以这么认为: EIGRP 的自动汇总只对本地产生的路由有效, 对学来的路由无效。读者可以关闭 HQ 路由器的自动汇总, 打开 Branch 路由器的自动汇总, 来验证这一结论。

8. 解: C

题目问: 哪一个地址和掩码组合表示 EIGRP 学来路由的汇总? 这道题考的是路由的汇聚, 要求对 192.168.25.20/30、192.168.25.16/30、192.168.25.24/30、192.168.25.28/30 进行汇总, 将它们换算成二进制的形式, 然后找出相同的位数, 就可以得到 192.168.25.16/28, 即 192.168.25.16 255.255.255.240。

9. 解: B

题目问: IP 地址和路由协议的配置如图所示, 网络管理员在 Router1 路由器上使用“show ip eigrp neighbors”命令, 输出显示在图中拓扑的下方, 问哪一个语句是正确的? 配置正确后, Router1 应该有 2 个 EIGRP 邻居, 可图中只有 Router2 一个邻居, Router3 没有出现在邻居表中, 从图中可以看到, 在 R3 上只通告了 192.168.2.0 和 10.0.0.0 的网段, 即只激活了接口 S1 和 10.0.4.0 的接口, 而接口 S0 没有被激活, 因此 R3 与 R1 之间是无法建立邻居的。解决的办法是在 Router3 的路由进程中添加 192.168.3.0 网络。

第 8 章

OSPF***

本章主要介绍链路状态路由协议的特点，OSPF 的特性、术语、包类型、邻居关系的建立、RID 的选择、DR 和 BDR 的选举、度量值的计算，以及 OSPF 的基本和高级配置等。



8.1 链路状态路由协议**

本节介绍链路状态路由协议特点、工作过程和优缺点。

8.1.1 链路状态路由协议介绍**

链路状态路由协议是复杂的、可扩展的路由选择协议。链路状态路由协议使用 Dijkstra 算法，也被称为 SPF（Shortest Path First，最短路径优先）算法。而距离矢量路由协议使用的是 Bellman-Ford 算法，高级的距离矢量路由协议 EIGRP 使用的是 DUAL 算法。

前面介绍了距离矢量路由协议 RIP 和高级的距离矢量路由协议 EIGRP，距离矢量路由协议就像是交通标志，仅仅给出方向和距离，根据指引一步一步地接近目的地，但并不知道整个网络的拓扑是什么样的。而链路状态路由协议更像是一幅地图，在地图中，可以看到所有的潜在路线，并确定首选的路径。

距离矢量路由有时也称为传闻路由，即相信其他路由器通告的路由都是真实的。在图 8-1-1 中，假设运行的是 RIP 协议，R1 应该把数据包发往 R2，然后再经 R3 到达网络 A，可是如果 R4 告诉 R1，从 R4 走只需要

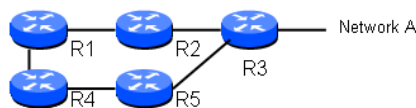


图 8-1-1 路由协议比较

1 跳，此时 R1 将把去往网络 A 的数据包转发给 R4，然后经 R5 和 R3 再到达网络 A。从这里可以看出距离矢量路由协议没有全局认识，仅根据相邻路由器发过来的信息进行路径选择。

链路状态路由协议采取一种不同的做法，看起来更像一个路线图。链路状态路由协议收集整个网络的拓扑信息，并基于这个拓扑信息决定到每一个网络的最短路径。感觉距离矢量路由协议就像是根据公路上的路标开车，可能要走弯路，而链路状态路由协议就像是看着地图，自己判断，并选择一条最佳的路径。

常见的链路状态路由协议有 OSPFv2 和 IS-IS。本书中提到的 OSPF 如没有特指，均指 OSPFv2。OSPFv3 是针对 IPv6 的，向后不兼容 IPv4。

8.1.2 链路状态路由协议工作过程**

在收敛过程中，所有的链路状态路由器将执行下面的过程。

- ① 每台路由器学习自己的链路，也就是激活的直接相连的网络。

② 每台路由器和直接相连的路由器进行交互。路由器间相互发送 Hello 报文，建立邻居关系。

③ 每台路由器构建包含直接相连的链路状态的 LSA（Link-State Advertisement，链路状态通告）。LSA 中记录了所有相关的路由器，包括邻居路由器的标识、链路类型和带宽等。

④ 每台路由器泛洪 LSA 给所有的邻居，路由器在数据库中存储所有收到的 LSA。邻居路由器再泛洪收到的 LSA 给自己的所有邻居，直到在同一个区域内的所有路由器都收到了所有的 LSA。每台路由器在本地数据库中保存所有收到的 LSA 的拷贝，被称为 LSDB（Link-State Database，链路状态数据库）。

⑤ 每台路由器基于本地的链路状态数据库（LSDB），然后执行 SPF 算法，以本路由器为树根，生成一个 SPF 树，基于 SPF 树，计算到每一个目的网络的最短路径，也就是路由表。链路状态路由协议路由表的生成过程如图 8-1-2 所示。

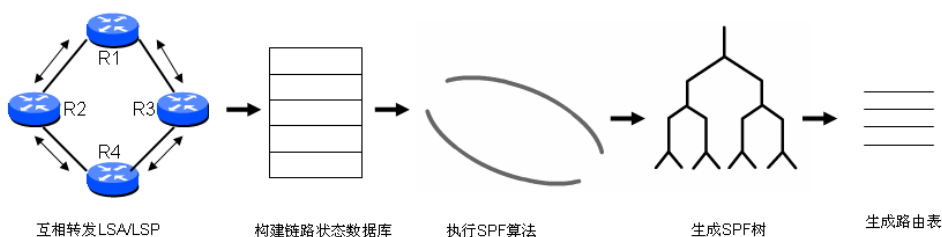


图 8-1-2 链路状态路由协议路由表的生成过程

8.1.3 链路状态路由协议的优缺点**

链路状态路由协议与距离矢量路由协议相比，有以下几个优点。

- **构建的是拓扑表：**运行链路状态路由协议的路由器间相互交换 LSA，形成 LSDB，SPF 算法基于 LSDB 构建网络的 SPF 树，使用 SPF 树，每台路由器可以独立地决定去往每个目标网络的最短路径。而距离矢量路由协议仅是根据邻居路由器的宣告来生成自己的路由表。说白了，就是链路状态路由协议有全局观念，距离矢量路由协议则显小农意识。
- **快速收敛：**运行链路状态路由协议的路由器收到 LSA 时，路由器立即泛洪该 LSA 到除接收端口以外的所有端口，然后本路由器再执行 SPF 算法，更新本地的路由表。而运行距离矢量路由协议的路由器收到邻居路由器的路由表时，先更新本地的路由表，然后再把新的路由表发送出去。这里提到的距离矢量路由协议都不包括 EIGRP，EIGRP 是一个高级的距离矢量路由协议，有更快的收敛速度。
- **事件驱动更新：**运行链路状态路由协议的路由器当检测到拓扑发生变化时才发送更新。而距离矢量路由协议的路由器是周期性更新，这里也不包括 EIGRP。这里要特别说明一点，执行 OSPF 的路由器每 30 分钟会泛洪一次 LSA，称为链路状态刷新，主要是用于 LSA 的老化机制。当 LSA 通告驻留在路由器的链路状态数据库中时，它们的老化时间是增大的，如果这些 LSA 通告达到了最大老化时间（1 个小时），那么它们将被从 OSPF 域中删除掉。所以要有一个机制来防止正常的 LSA 到达老化时间时被清掉，每隔 30 分钟，始发这条 LSA 通告的路由器就将泛洪这条 LSA 的一个新拷贝，并将它的序列号加 1，老化时间设置为 0。读者知道有这么一个 30 分钟就可以了，但不要错误地把 OSPF 理解成周期性更新。

- **层次型设计**：运行链路状态路由协议的路由器，都有一个区域的概念。多个区域可以方便路由的汇总，把一些路由的问题限制在一个区域内。区域的 OSPF 和 IS-IS 将在 CCNP 部分讨论，CCNA 部分仅讨论单个区域 OSPF 的配置。

链路状态路由协议与距离矢量路由协议相比，有以下几个缺点，更合适的应该说需求。

- **内存需求**：运行链路状态路由协议的路由器需要更多的内存来保存链路状态数据库。
- **处理器需求**：运行链路状态路由协议的路由器需要执行 SPF 来构建网络拓扑图，需要更强的 CPU。
- **带宽需求**：在网络初始化时，大量链路状态包的泛洪，会影响网络的可用带宽。在不稳定的网络中，链路状态包的泛洪也会影响网络的可用带宽。

现在很多做法是把链路状态路由协议划分成更小的区域，来减小链路状态数据库的大小和限制 LSA 的泛洪，从而降低对内存、CPU 和带宽的需求。



8.2 OSPF 概述和基本配置***

本节介绍 OSPF 术语、包格式、包类型、邻居关系的建立、DR 和 BDR 的选举、度量值的计算等。

8.2.1 OSPF 特性***

OSPF (Open Shortest Path First, 开放最短路径优先) 是一个开放标准的路由选择协议，被各种网络开发商广泛支持，其中包括思科的路由器和交换机，可以这么说，OSPF 是目前使用最广泛的 IGP 路由协议。RIPv1 和 RIPv2 收敛速度较慢，在大型复杂的网络中还容易带来路由环路问题；IGRP 和 RIPv1 一样，也是有类路由协议，不支持 VLSM 和 CIDR，同样有距离矢量路由协议的缺点，现在基本上退出历史舞台，也退出了 CCNA 考试范畴；EIGRP 是一个高级的距离矢量路由协议，虽然支持 VLSM 和 CIDR，并能快速收敛，也不会产生路由环路，但它是一个私有协议，仅能应用在思科公司的设备上。

OSPF 是一个链接状态路由协议，采用 SPF 算法（也称为 Dijkstra 算法），在同一个区域内的所有路由器交换 LSA，构建 LSDB，每台路由器以本路由器为根，基于 LSDB 执行 SPF 算法，生成 SPF 树，计算到每个目的地的最短路径，产生路由表。

作为链接状态路由协议，OSPF 具有以下特性：

- **IETF 标准**。意味着 OSPF 可以被不同厂商的设备所支持。
- **无环路由协议**。执行的是 SPF 算法，不会产生路由环路。
- **无类路由协议**。支持 VLSM 和 CIDR。
- **拥有不受限的跳计数**。可以应用于大型网络。
- **层次型**。易扩展，路由器的负担不会随着网络规模的增大而急剧增加。
- **区域化设计**。减小路由更新的流量，降低内存、CPU 和带宽的使用。
- **快速收敛**。使用触发式更新，路由可以快速收敛。
- **支持验证**。OSPF 支持针对区域和链路的验证。

8.2.2 OSPF 术语**

1. 链路 (Link)

当一个接口被加入到 OSPF 进程中时，它就被认为是 OSPF 的一个链路。

2. 链路状态 (Link-State)

链路的状态信息，包括接口的 IP 地址和子网掩码、接口的网络类型（比如是广播式的以太网，还是串行的点对点，或是其他链路）、链路的花费（根据接口的带宽进行计算）、链路上的邻居。

3. 路由器 ID (Router ID, 简称 RID)

路由器 ID 是一个来标识此路由器的 IP 地址，可以在 OSPF 路由进程中手工指定；如果没有指定，路由器选择所有环回接口中最高的 IP 地址作为路由器 ID；如果没有环回接口被使用，路由器将选择所有激活的物理接口中最高的 IP 地址作为路由器 ID。

4. 邻居 (Neighbor)

两台或更多台路由器连接在一个公共的网络上，如两台路由器通过串行接口相连，多台路由器通过以太网接口相连。

5. 邻接 (Adjacency)

邻接是两台路由器之间的关系，这两台路由器允许直接交换路由更新数据。OSPF 只与建立了邻接关系的邻居共享路由信息。并不是所有的邻居都可以成邻接关系，这要取决于网络的类型和路由器的配置；并不是有邻接关系的路由器都是邻居，CCNP 中会涉及虚电路，两台路由器并不是直接相连，也可以共享路由信息。

6. 区域 (Area)

OSPF 通过划分区域来实现分层设计。OSPF 是以链路划分区域的，在图 8-2-1 中，同一个 AS（自治系统）内的路由器被划分在 3 个 OSPF 区域内，路由器 R2 和 R3 跨越两个区域，它们被称为 ABR（Area Border Router，区域边界路由器）。所有的区域都与 Area 0 相连，Area 0 被称为骨干区域，骨干区域路由器具有整个 AS 的所有路由条目，对路由器的配置要求相对较高。而其他区域可以是标准区域，也可以是某些特殊区域，里面可以仅有 AS 内的部分路由，对路由器的配置要求相对较低。通过划分区域，将 LSA 扩散限制在区域内，进而可以减少每个区域内路由表条目，还可将区域内的拓扑变化的影响限制在本区域内。CCNA 中仅涉及单区域的 OSPF，多区域 OSPF 是 CCNP 部分的内容。

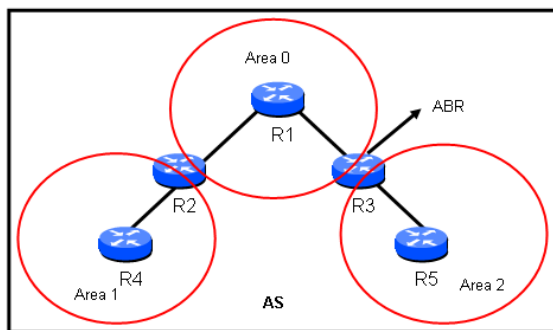


图 8-2-1 多区域的 OSPF

7. 指定路由器 (Designated Router, 简称 DR)

当 OSPF 路由器被连接到多路访问的网络中的时候，需要选择一台指定路由器 (DR)，

该路由器代表该多路访问网络中的所有路由器，每台路由器都把拓扑变化发往 DR 和 BDR。然后由 DR 通知该多路访问网络中的其他路由器。

8. 备用的指定路由器（Backup Designated Router，简称 BDR）

备用的指定路由器，当 DR 因故障离线时，BDR 转变成 DR，接替 DR 的工作。

9. 花费（Cost）

每条链路都有一个花费。花费是根据链路的带宽计算而来的，并可以人为地修改。OSPF 使用的唯一度量值就是花费。

8.2.3 OSPF 包格式*

OSPF 和 EIGRP 一样，也被设计成一个网络层协议，协议号是 89。OSPF 的包格式如图 8-2-2 所示。

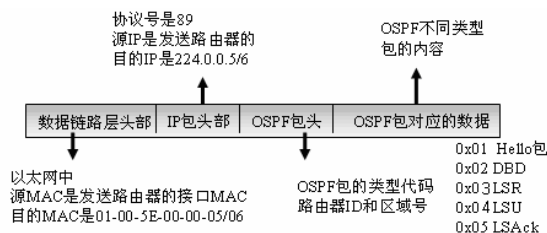


图 8-2-2 OSPF 的包格式

包括：

- **数据链路层头部：**OSPF 使用的组播 IP 地址是 224.0.0.5（非 DR 和 BDR 路由器使用的地址）和 224.0.0.6（DR 和 BDR 路由器使用的地址），每个组播 IP 地址都有对应的 MAC 地址，组播 MAC 地址的厂商编码部分固定为“01-00-5E”，编号部分从具体的组播 IP 地址计算而来。224.0.0.5 和 224.0.0.6 对应的 MAC 地址是“01-00-5E-00-00-05”和“01-00-5E-00-00-06”。
- **IP 包头部：**协议号是 89，源 IP 地址是发送路由器的 IP 地址，目的 IP 地址是 224.0.0.5 或 224.0.0.6。
- **OSPF 头部：**包括路由器 ID 和所在的区域号，以及 OSPF 包的类型代码。OSPF 包括 5 种包，稍后介绍 5 种包的用途。
- **OSPF 包对应的数据：**每种类型包的具体内容。

8.2.4 OSPF 包类型***

重点是 Hello 包和 LSU 的分类，下面结合基本配置讲解 Hello 包。

OSPF 有 5 种不同类型的链路状态包（Link_State_Packet，LSP），每一种包都有特定的用途。这 5 种包是：

1. Hello

Hello 报文被用来建立和维护 OSPF 路由器间的邻接关系。OSPF 的 Hello 报文的作用主要有：发现 OSPF 邻居，建立和维护邻接关系；在多路访问的网络中选择 DR 和 BDR。什么是多路访问的网络？在稍后的 OSPF 网络类型中介绍。

OSPF 泛洪链路状态通告给其他路由器之前，需要先建立邻接关系。路由器在所有启用 OSPF 协议的接口上发送 Hello 报文，以判断是否有其他 OSPF 路由器运行在相同的链路上，Hello 报文一般以组播方式发送，组播的地址是 224.0.0.5。相邻的路由器能否建立邻接关系取决于 OSPF 的 Hello 报文，OSPF 报头和 Hello 报文的格式如图 8-2-3 所示。

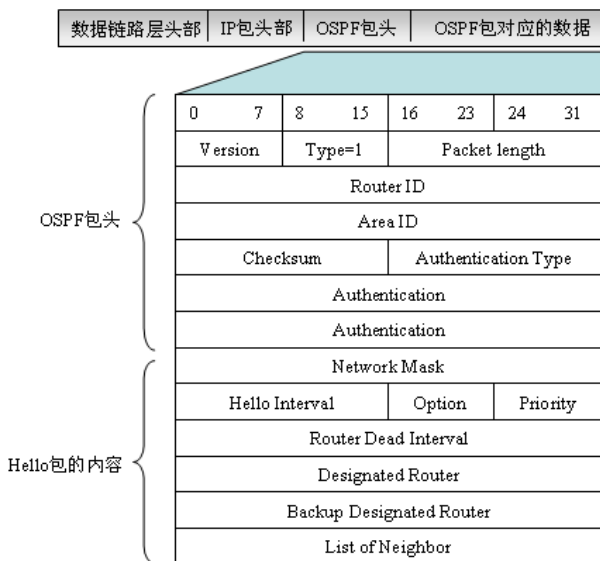


图 8-2-3 Hello 报文格式

CCNA 考生并不需要了解 OSPF 报头和 Hello 报文的格式，但了解 OSPF 报头和 Hello 报文中的一些关键字段，有助于加强对 OSPF 的理解。OSPF 报头和 Hello 报文包含的字段如下：

- **Version:** OSPF 的版本号，当前使用的是 OSPFv2。OSPFv1 是一个实验版本，早已淘汰，OSPFv3 是针对 IPv6 的。
- **Type=1:** 类型 1 的报文是 Hello 报文，类型 2 是 DBD，类型 3 是 LSR，类型 4 是 LSU，类型 5 是 LSAck。
- **Packet Length:** 报文长度。
- **Router ID:** 路由器 ID，是每台路由器的唯一标识。
- **Area ID*:** 区域号，CCNA 中只介绍单区域的 OSPF，一般配置的都是区域 0。
- **Checksum:** 校验和。
- **Authentication Type*:** 验证类型。0 表示不使用验证，1 表示明文验证，2 表示 MD5 验证。
- **Authentication:** 验证相关信息，包括密码等。
- **Hello Interval:** Hello 时间间隔。
- **Option:** 选项信息。
- **Priority:** OSPF 路由器的接口优先级，主要用于 DR 和 BDR 的选举。
- **Router Dead Interval:** 路由器死亡间隔。
- **Designated Router:** DR，指定路由器的 Router ID。
- **Backup Designated Router:** BDR，备用的指定路由器的 Router ID。

- List of Neighbor: 邻居列表。

相邻的 OSPF 路由器要建立邻接关系, Hello 报文中的区域号, Hello 间隔和死亡间隔必须相同, 此外如果有验证, 验证也要相同, CCNP 中还会涉及区域类型, 区域类型也要一致。CCNA 考试中只涉及单一区域的 OSPF, 考生重点关注 Hello 间隔和死亡间隔是否一致, 验证是否相同就可以了。这一点与 EIGRP 不同, EIGRP 要建立邻接关系, 只要 AS 号和 K 值相同就可以了, 对 Hello 间隔和死亡间隔没有要求。

OSPF 支持的网络类型有:

- Point-to-point, 点对点, 最典型的的就是串行线路。
- Broadcast Multiaccess, 广播的多路访问, 最典型的就是以太网。
- NonBroadcast MultiAccess (NBMA), 非广播的多路访问, 最典型的就是帧中继。
- Point-to-multipoint, 点对多点, 属于 CCNP 的内容。
- Virtual links, 虚电路, 两台路由器间不需要直接相邻, 也能建立起邻接关系, 也属于 CCNP 的内容。

CCNA 只要掌握 OSPF 在点对点的串行线路和多路访问的以太网中的配置就可以了。在不同的网络类型中, OSPF 的 Hello 间隔也不相同。在默认情况下, 在广播和点对点链路中, 默认的 Hello 间隔是 10 秒; 在 NBMA 的网络上是 30 秒。死亡间隔是 Hello 间隔的 4 倍。

路由器的 Hello 间隔和死亡间隔可以通过下面的命令进行修改:

```
Router(config)#int s1/1
Router(config-if)#ip ospf hello-interval 20 把Hello间隔改成20秒。
Router(config-if)#ip ospf dead-interval 60 把死亡间隔改成60秒。
```

2. DBD (Database Description, 数据库状态描述包)

DBD 是发送路由器链路状态数据库的一个简短描述, 可以理解成提纲或目录, 接收路由器用此信息与本地的链路状态数据库作对比, 检测发送端和接收端的链路状态数据库是否同步。

3. LSR (Link-State Request, 链路状态请求包)

接收路由器可以发送 LSR 来请求发送路由器 DBD 中的某些条目的详细信息。

4. LSU (Link-State Update, 链路状态更新包)

LSU 被用来更新 OSPF 路由信息, 回复 LSR 请求。LSU 被分成多种类型的 LSA (Link-State Advertisement, 链路状态通告), 比如类型 1 的 LSA 是 Router LSA, 类型 2 的 LSA 是 Network LSA 等, LSA 类型的讨论属于 CCNP 的内容。

LSP 和 LSA 比较容易混淆, 严格来说, LSP 有 5 种类型, 包括 Hello、DBD、LSR、LSU、LSAck; 而 LSU 又被细分成各种 LSA, 譬如类型 1、类型 2 等。有时这两个概念也被互换使用。

5. LSAck (Link-State Acknowledgement, 链路状态确认)

当一个 LSU 被收到时, 路由器发送 LSAck 进行确认。

8.2.5 OSPF 邻居关系的建立**

OSPF 邻居关系的建立需要经历多个阶段, 如图 8-2-4 所示。

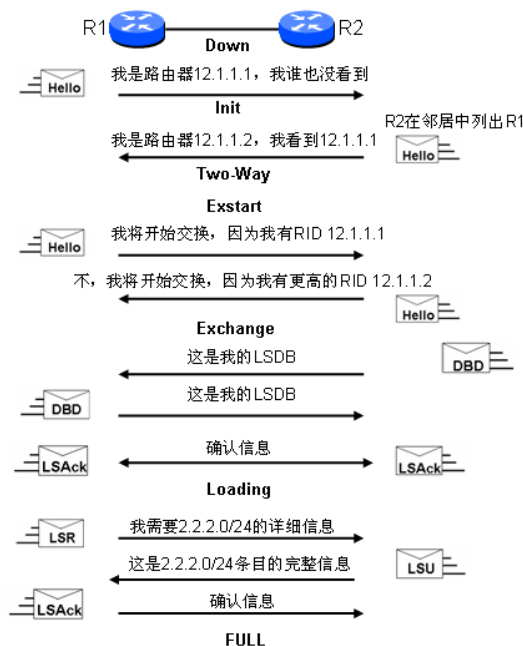


图 8-2-4 OSPF 邻居关系的建立过程

- **Down:** OSPF 路由器的初始状态，在 Down 状态下，OSPF 进程还没有与任何邻居交换信息。
 - **Init:** 初始化阶段，表示已经收到了邻居路由器的 Hello 报文，但是该报文列出的邻居中没有发现本路由器的 Router ID，也就是说，对方并没有收到本路由器发出的 Hello 报文。
 - **Two-Way:** 双向阶段，表示双方互相收到了对方发过来的 Hello 报文，建立了邻居关系。在多路访问的网络中，两个接口状态是 DROther 的路由器之间将停留在此状态，其他情况将继续转入后续状态。Two-Way 状态是 OSPF 邻居之间最基本的关系，但处在这种关系中的路由器之间是不能共享路由信息的，要想共享路由信息，路由器间需要建立邻接的关系。
 - **Exstart:** 准备开始交换阶段，路由器之间用 Hello 分组来协商它们之间的主/从关系，有最高 Router ID 的路由器成为主路由器。当邻居路由器建立了它们之间的主从角色后，它们就进入了 Exchange 状态并开始发送路由选择信息。
 - **Exchange:** 开始交换阶段，路由器将本地的 LSDB 用 DBD (DataBase Description, 数据库描述) 报文来描述，并发给邻居。如果任何一台路由器收到不在其数据库中的有关链路的信息，该路由器就向其邻居请求有关该链路的完整信息。完整的路由信息在 “Loading” 状态下交换。
 - **Loading:** 加载阶段，路由器发送 LSR 报文向邻居请求对方的路由条目的详细信息。当路由器收到一个 LSR 时，它会用 LSU 进行回应。LSU 中含有确切的 LSA，收到 LSU 的路由器需要使用 LSAck 对发送 LSU 的路由器进行确认。
 - **Full:** 完全邻接状态，Loading 状态结束后，路由器就变成 Full adjacency。
- CCNA 考生没有必要掌握邻接建立的详细过程，对此有个大概的了解就可以了。

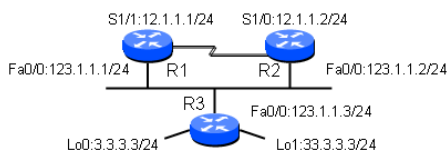


图 8-2-5 有 DR 和 BDR 的多路访问网络

8.2.6 OSPF 基本配置***

1. 配置

使用 OSPF 协议配置如图 8-2-5 所示的网络。

R1 的配置和解释如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#no cdp run
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int fa 0/0
R1(config-if)#ip add 123.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#router ospf 1
```

启用 OSPF 协议，这里的 1 是进程号（process-id），进程号的取值范围是 1~65535。这里的进程号仅具有本地意义，与同一个区域中的 OSPF 路由器进程号没有关系，进程号不同不影响邻接关系的建立。EIGRP 协议后面跟的是 AS 号，不同的 EIGRP 要想交互路由信息，AS 号必须相同。注意本实验中路由器 R3 的 OSPF 进程号就与 R1 的不同。

```
R1(config-router)#network 12.1.1.0 0.0.0.255 area 0
```

宣告网络，这里的 Network 命令与 EIGRP 的配置相似，也使用了 IP 子网和反掩码的格式。任何在此 IP 地址范围内的接口都运行 OSPF 协议，发送和接收 OSPF 报文。OSPF 向外通告在此地址范围内的接口所在的 IP 网络号。IP 子网和反掩码有多种输入形式，下面分别演示。“area 0”指的是区域号，前面介绍了 OSPF 可以采用多区域来实现分层设计，一台路由器的不同接口可以属于多个 OSPF 区域，相邻路由器的接口要在同一个区域内才能建立邻接关系。CCNA 中仅涉及单区域的配置。

```
R1(config-router)#net 123.1.1.1 0.0.0.0 area 0
```

这里使用的是一种变化格式，“0.0.0.0”的反掩码限制只有一个 IP 地址可以满足，也就是 IP 地址是 123.1.1.1 的接口运行 OSPF 协议，OSPF 向外宣告该接口的网络号。这属于一种非正规写法，参加 CCNA 考试的考生请使用前面介绍的规范格式。

R2 的配置和解释如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#no cdp run
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int fa 0/0
R2(config-if)#ip add 123.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#router ospf 1
R2(config-router)#network 0.0.0.0 0.0.0.0 area 0
```

如果一台路由器的所有接口都运行 OSPF，可以使用这种简化的方式。使用“show run”命令查看配置时，可以发现此命令自动被修改成“network 0.0.0.0 255.255.255.255 area 0”。为了节省时间，输入 8 个 0 更方便。

R3 的配置和解释如下：

```
Router>en
Router#conf t
Enter configuration commands,
one per line. End with CNTL/Z.
Router(config)#host R3
R3(config)#no cdp run
R3(config)#int fa 0/0
R3(config-if)#ip add 123.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
```

```
R3(config-if)#int lo1
R3(config-if)#ip add 33.3.3.3 255.255.255.0
R3(config-if)#router ospf 3
```

注意这里的 OSPF 进程号是 3。与不同 OSPF 路由器的进程号没有关系，进程号仅具有本地意义。

```
R3(config-router)#net 3.3.3.3 255.255.255.0 area 0
```

这里仍然是不规范输入，直接输入接口的 IP 地址和正向子网掩码，查看配置时，可以发现此命令自动被修改成规范格式“network 3.3.3.0 0.0.0.255 area 0”，这种输入方式省去了用户计算反向子网掩码的时间。

```
R3(config-router)#network 123.1.1.0 0.0.0.255 area 0
```

2. 查看

(1) 路由表

在路由器 R1 上查看路由表，显示如下：

```
R1#show ip route
 3.0.0.0/32 is subnetted, 1 subnets
O    3.3.3.3 [110/2] via 123.1.1.3, 00:26:35, FastEthernet0/0
 123.0.0.0/24 is subnetted, 1 subnets
C    123.1.1.0 is directly connected, FastEthernet0/0
 12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/1
```

从上面的输出中，可以看到 R1 学到了 R3 上 Loopback 0 接口的 IP 子网。“O 3.3.3.3 [110/2] via 123.1.1.3, 00:26:35, FastEthernet0/0”，这里的“O”表示的是 OSPF，该路由是通过 OSPF 学来的。从父路由“3.0.0.0/32”中，可以知道 R1 学到的是 3.3.3.3/32 的路由，是一个 32 位的主机路由。在 OSPF 中，所有环回接口都自动被宣告成 32 位的主机路由，而忽略接口实际的子网掩码，如果想显示环回接口真实的子网掩码，可以在环回接口下使用下面的命令：

```
R3(config)#int lo0
R3(config-if)#ip ospf network point-to-point
```

“[110/2]”这里的 110 是 OSPF 的管理距离，2 是 OSPF 的度量值。“via 123.1.1.3”是路由下一跳的 IP 地址，“00:26:35”是路由存在的时间，“FastEthernet0/0”是本路由器的外出接口。从这里看到与 RIPv2 和 EIGRP 协议的一点不同是，OSPF 不支持自动汇总。OSPF 支持手工汇总，OSPF 的手工汇总要在区域的边界上执行，CCNA 中只涉及单区域的 OSPF 配置，也就讨论不到手工汇总问题了。

R1 学不到 R3 Loopback 1 接口的路由，原因是因为 R3 没有宣告该接口。

(2) 邻居表

在路由器 R1 上查看邻居表，显示如下（读者看到的结果可能会与这里显示的不同，这里是先配置 R2 的 OSPF，再配置 R1 的 OSPF，最后配置 R3 的 OSPF 得到的结果）：

```
R1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.3.3.3	1	FULL/DROTHER	00:00:34	123.1.1.3	FastEthernet0/0
123.1.1.2	1	FULL/DR	00:00:39	123.1.1.2	FastEthernet0/0
123.1.1.2	0	FULL/-	00:00:39	12.1.1.2	Serial1/1

- **Neighbor ID:** 指的是邻居路由器的 Router ID。从这里的输出可以看到，R3 的 RID 是 33.3.3.3，R2 的 RID 是 123.1.1.2。R1 和 R2 通过不同接口建立了两次邻居关系。
- **Pri:** OSPF 邻居接口的优先级，接口优先级主要用于 DR 和 BDR 的选举。以太网接口需要选举 DR 和 BDR，接口的优先级默认是 1。点对点链路不需要选举 DR 和 BDR，接口的优先级是 0。可以在路由器上使用“show ip ospf interface”命令查看接口的优先级，R1 的显示如下：


```

R1#show ip ospf interface fa 0/0
FastEthernet0/0 is up, line protocol is up
Internet Address 123.1.1.1/24, Area 0
Process ID 1, Router ID 123.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 123.1.1.2, Interface address 123.1.1.2
Backup Designated router (ID) 123.1.1.1, Interface address 123.1.1.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

```

从上面的输出中,可以发现很多信息。路由器 R1 Fa0/0 接口所在的区域是 Area 0, OSPF 的进程号是 1,路由器的 RID 是 123.1.1.1,网络类型是广播,接口花费是 1。本路由器在这个以太网段的角色是 BDR,接口的 OSPF 优先级是 1,该网段的 DR 是 123.1.1.2,该以太网接口的 Hello 间隔是 10 秒,死亡时间是 40 秒。

- **State:** 邻居路由器的状态。“FULL”表示已经建立了邻接关系,R3 是 DROther,R2 是 DR,本路由器是 BDR。在点对点链路上没有 DR 和 BDR 的选举,显示的是“-”。
- **Dead Time:** 显示邻居的死亡时间,如果该值减小到 0,邻居消失。该值默认是 Hello 间隔的 4 倍。
- **Address:** 邻居直连接口的 IP 地址。
- **Interface:** 本路由器的外出口口。

从上面的输出中,可以看到 R1 有 3 个邻居,并且都建立了邻接关系。

(3) 拓扑表

拓扑表也就是链路状态数据库,在路由器 R1 上查看拓扑数据库,显示如下:

```

R1#show ip ospf database

OSPF Router with ID (123.1.1.1) (Process ID 1)

Router Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum Link count
33.3.3.3     33.3.3.3     317         0x80000002  0x004F74  2
123.1.1.1    123.1.1.1    978         0x8000000F  0x006D81  3
123.1.1.2    123.1.1.2    1237        0x80000010  0x0010DA  3

Net Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum
123.1.1.2    123.1.1.2    284         0x80000007  0x008F79

```

CCNA 中不要求对拓扑数据库有过多了解。读者可以在 R2、R3 上查看拓扑数据库,3 台路由器的拓扑数据库一样,在同一个区域内的所有 OSPF 路由器的拓扑数据库都是一样的。

不要关闭路由器,继续下面的实验。

8.2.7 DR 和 BDR***

1. 为何要选择 DR 和 BDR

在如图 8-2-6 所示的多路访问网络中,5 台路由器接在同一个以太网中。假设没有 DR 和 BDR 的情况下,为了交互路由,每台路由器都要与其他路由器建立邻接关系。每台路由器都需要与其他 4 台路由器建立邻接关系,图中需要建立 $n*(n-1)/2$ 个邻接关系,其中 $n=5$,也就是总共需要建立 10 个邻接关系。如果有一台路由器离开,要和所有的路由器断开邻接;如果有一台新的路由器加入,要和所有的路由器新建邻接。这样不仅影响收敛的速度,也占用网络的带宽。

在如图 8-2-7 所示的多路访问网络中，选举了 DR 和 BDR，所有的 DROther（除 DR 和 BDR 之外）路由器都与 DR 和 BDR 建立邻接关系，DROther 路由器之间停留在 Two-Way 状态，路由器邻接关系的减少，可以加速网络的收敛。如果网络上有更新的路由条目，DROther 路由器向组播地址 224.0.0.6 发出。224.0.0.6 是 DR 和 BDR 的组播地址，DROther 路由器使用的组播地址是 224.0.0.5。DR 用 224.0.0.5 的组播地址向全部的网络发送 LSA，避免使用单播分别通知各个路由器，这样减少了网络带宽的占用，从而更有效地利用带宽资源。如果有路由器离开，这个路由器也只与 DR 和 BDR 建立了邻接关系，由 DR 通告 LSA 信息来达到网络的快速收敛。

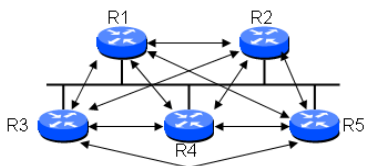


图 8-2-6 没有 DR 和 BDR 的多路访问网络

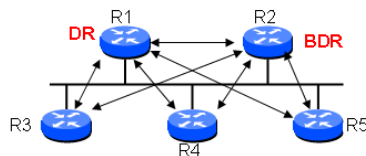


图 8-2-7 有 DR 和 BDR 的多路访问网络

从上面的分析中可以看出，在多路访问的网络中需要选举 DR 和 BDR。广播型多路访问的网络有以太网、令牌环和 FDDI；非广播型多路访问的网络有帧中继、X.25 和 SMDS。广播和非广播多路访问的网络都属于多路访问的网络，需要选举 DR 和 BDR。

点对点（PPP 或 HDLC 封装）或点对多点（由管理员手工配置）的网络中不需要选举 DR 和 BDR。

2. Router ID 选举

Router ID 简称 RID，被用来唯一标识 OSPF 域中的每一台路由器。如果两台 OSPF 路由器的 RID 一样，彼此间无法建立邻接关系。RID 是以 IP 地址的形式出现的，在思科路由器上按照下面的 3 种顺序来选举 RID。

① router-id 配置命令最优先。在路由器 R3 上使用“show ip protocols”命令，查看运行的 IP 协议，显示如下：

```
R3#show ip protocols
Routing Protocol is "ospf 3"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 33.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    3.3.3.0 0.0.0.255 area 0
    123.1.1.0 0.0.0.255 area 0
  Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    123.1.1.2        110           00:42:15
    123.1.1.1        110           00:42:15
  Distance: (default is 110)
```

这里显示路由器的 Router ID 是 33.3.3.3。下面手工配置路由器 R3 的 Router ID。

```
R3(config)#router ospf 3          进入路由配置模式。
R3(config-router)#router-id 8.8.8.8 手工配置 Router ID。
Reload or use "clear ip ospf process" command, for this to take effect
系统提示要使配置的 Router ID 生效，需要重启路由器或重启 OSPF 进程。重启 OSPF 进程的命令是 "clear ip ospf process"。
```

```
R3(config-router)#^Z
R3#clear ip ospf process
Reset ALL OSPF processes? [no]: y
```

确定重启 OSPF 进程。

路由器的控制台上会出现下面的提示：

```
*Mar 1 04:11:35.946: %OSPF-5-ADJCHG: Process 3, Nbr 123.1.1.1 on FastEtherne 0
from FULL to DOWN, Neighbor Down: Interface down or detached
*Mar 1 04:11:35.946: %OSPF-5-ADJCHG: Process 3, Nbr 123.1.1.2 on FastEthernet0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
*Mar 1 04:11:36.218: %OSPF-5-ADJCHG: Process 3, Nbr 123.1.1.1 on FastEthernet0/0 from
LOADING to FULL, Loading Done
*Mar 1 04:11:38.934: %OSPF-5-ADJCHG: Process 3, Nbr 123.1.1.2 on FastEthernet0/0 from
LOADING to FULL, Loading Done
```

上面的提示显示路由器 R3 与 R1 和 R2 的邻居关系 down 掉，然后又重新建立邻接。再次查看 R3 的 Router ID，显示如下：

```
R3#show ip protocols
Routing Protocol is "ospf 3"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 8.8.8.8
```

从上面的输出中可以发现，路由器 R3 的 Router ID 已经变成了 8.8.8.8。从中读者还发现，OSPF 路由器的 Router ID 可以是一个并不存在的 IP 地址，更不需要路由可达。Router ID 仅仅标识路由器的名字，不用于路径的寻址。

② 如果没有使用 Router ID 命令指定，OSPF 路由器选择最大激活的环回接口的 IP 地址作为 Router ID。路由器 R3 的配置如下：

```
R3(config)#router ospf 3
R3(config-router)#no router-id 删除之前手工指定的 Router ID。
Reload or use "clear ip ospf process" command, for this to take effect
R3(config-router)#int lo1
R3(config-if)#shut 关闭 Loopback 1, 该接口的 IP 地址 33.3.3.3 将不会成为 Router
ID, 因为该接口不是一个激活的端口。

R3(config-if)#^Z
R3#clear ip ospf process
Reset ALL OSPF processes? [no]: y
```

再次查看 R3 的 Router ID，显示如下：

```
R3#show ip protocols
Routing Protocol is "ospf 3"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
```

从上面的输出中可以看出，R3 的 Router ID 是 3.3.3.3。

③ 如果 OSPF 路由器没有激活的环回接口，路由器选择最大激活的物理接口的 IP 地址作为 Router ID。这里优先使用环回接口，是因为环回接口比物理接口更稳定，除非手工关闭接口，否则只要路由器正常运行，环回接口就一直有效。路由器 R3 的配置如下：

```
R3(config)#int lo0
R3(config-if)#shut 关闭 Loopback 0 接口。
R3(config-if)#int s1/2 配置一个没有连线的物理接口。
R3(config-if)#ip add 192.168.1.1 255.255.255.0
配置一个比 123.1.1.3 更大的 IP 地址，但不激活该端口。
R3(config-if)#^Z
R3#clear ip ospf process 重启 OSPF 进程。
Reset ALL OSPF processes? [no]: y
```

再次查看 R3 的 Router ID，显示如下：

```
R3#show ip protocols
Routing Protocol is "ospf 3"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
```

Router ID 竟然没有发生改变，重新启动 OSPF 路由器，或者清除 OSPF 配置，然后再重新配置。命令执行如下：

```
R3(config)#no router ospf 3
R3(config)#router ospf 3
R3(config-router)# log-adjacency-changes
显示邻居邻接关系的变化，是默认产生的配置，之所以能看到邻接关系的 down 和 up，都是该语句的作用。
R3(config-router)# network 3.3.3.0 0.0.0.255 area 0
R3(config-router)# network 123.1.1.0 0.0.0.255 area 0
```

再次查看 R3 的 Router ID，显示如下：

```
R3#show ip protocols
Routing Protocol is "ospf 3"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 123.1.1.3
```

路由器的 Router ID 变成最大激活物理接口的 IP 地址。

3. DR 和 BDR 选举

在图 8-2-5 中，路由器 R1、R2、R3 通过快速以太网连接在一起。在广播式多路访问的网络中，需要选举 DR 和 BDR。OSPF 路由器选举接口优先级最高的路由器为 DR，接口优先级次高的路由器为 BDR，如果接口优先级相同，将使用 Router ID，Router ID 高的路由器被选为 DR 或 BDR，除 DR 和 BDR 之外的路由器称为 DROther。

经过前面的配置和后来的调整，R1 的 Router ID 是 123.1.1.1，R2 的 Router ID 是 123.1.1.2，R3 的 Router ID 是 123.1.1.3，路由器接口的优先级都是默认的 1。根据前面的叙述，R3 应该是 DR，R2 应该是 BDR，R1 应该是 DROther，事实果真如此吗？在路由器 R3 上进行验证，显示如下：

```
R3#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
123.1.1.1	1	FULL/BDR	00:00:37	123.1.1.1	FastEthernet0/0
123.1.1.2	1	FULL/DR	00:00:38	123.1.1.2	FastEthernet0/0

从上面的输出中，却发现 R2 是 DR，R1 是 BDR，R3 是 DROther。为何会出现这样的结果呢？这是因为 OSPF 为了保障网络的相对稳定性，DR 和 BDR 的选举没有采用抢占机制。假设路由器 R1、R2、R3 同时启动了 OSPF 进程，根据 DR 和 BDR 选举顺序，各个接口的优先级都是默认的 1，接下来比较 Router ID，R3 的 Router ID 最大，成为 DR；R2 的 Router ID 次之，成为 BDR；R1 的 Router ID 最小，成为 DROther。事实上 R1、R2 和 R3 并没有同时启动 OSPF 进程，最先启动 OSPF 进程的路由器将会成 DR，其次启动 OSPF 进程的成为 BDR，最后启动 OSPF 进程的成为 DROther。这就是为什么 R2 是 DR，R1 是 BDR，R3 是 DROther 的原因。

接下来重启 R2 的 OSPF 进程。在路由器 R2 上执行：

```
R2#clear ip ospf process
Reset ALL OSPF processes? [no]: y
```

现在哪台路由器成为了 DR，哪台路由器成为了 BDR 呢？先来分析一下，R2 本来是 DR，现在 DR 离开。R1 将从 BDR 升级成为 DR，R3 从 DROther 升级成为 BDR。R2 的 OSPF

进程重新运行后，DR 和 BDR 都有归属，R2 只能成为 DROther 了。在路由器 R3 上验证，显示如下：

```
R3#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
123.1.1.1	1	FULL/DR	00:00:38	123.1.1.1	FastEthernet0/0
123.1.1.2	1	FULL/DROTHER	00:00:34	123.1.1.2	FastEthernet0/0

从上面的输出中，可以看出 R1 是 DR，R2 是 DROther，R3 应该是 BDR，结果证实了前面的分析。

假设 3 台路由器中，R1 的硬件配置非常高，想让 R1 永远是 DR，应该如何配置呢？前面提到了 DR 的选举顺序，首先考虑的是接口的优先级，可不可以把 R1 的 Fa0/0 接口的优先级设置成 2，来让该路由器永远成为 DR 呢？回答是否定，因为 OSPF 中 DR 和 BDR 的选举不采用抢占机制，严格按照资格老来排辈，如果 R1 重启或因其他原因离开再回来，网络中已经有了 DR 和 BDR，R1 就只能等 DR 和 BDR 都出问题以后，才能升级到 DR。

有一种让 R1 永远是 DR 的办法，那就是把网络中其他路由器接口的优先级都设成 0。优先级为 0 表示该接口不参与 DR 和 BDR 的选举。配置路由 R2 和 R3 如下：

```
R2(config)#int fa 0/0
```

```
R2(config-if)#ip ospf priority 0  把该接口的优先改成 0，不参与 OSPF 中 DR 和 BDR 的选举。
```

```
R3(config)#int fa 0/0
```

```
R3(config-if)#ip ospf priority 0
```

在路由器 R3 上查看 OSPF 邻居的情况，显示如下：

```
R3#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
123.1.1.1	1	FULL/DR	00:00:38	123.1.1.1	FastEthernet0/0
123.1.1.2	0	2WAY/DROTHER	00:00:34	123.1.1.2	FastEthernet0/0

从上面的输出中，可以看出 R1 是 DR，R3 和 R2 之间的关系停留在 2WAY 状态，并没有形成邻接关系，R2 和 R3 应该都是 DROther。在多路访问的网络中，所有路由器只与 DR 和 BDR 形成邻接关系。DROther 路由器间停留在 2WAY 状态，相互间不交互路由信息。

清除 R1 的 OSPF 进程后，再次查看 R1 上的邻居关系，显示如下：

```
R1#clear ip ospf process
```

```
Reset ALL OSPF processes? [no]: y
```

```
R1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
123.1.1.2	0	FULL/DROTHER	00:00:38	123.1.1.2	FastEthernet0/0
123.1.1.3	0	FULL/DROTHER	00:00:39	123.1.1.3	FastEthernet0/0
123.1.1.2	0	FULL/-	00:00:38	12.1.1.2	Serial1/1

从上面的输出中可以看出，R1 重启 OSPF 进程后，R1 仍然是 DR，R2 和 R3 仍然是 DROther，在 R1、R2 和 R3 的网络中没有 BDR。如果 R1 故障，R2 和 R3 之间将不能通过以太网正常交互路由信息。

有一个说法必须强调一下，DR 和 BDR 的选举是基于接口的，而不是基于路由器的。一台路由器可能是某一个网段的 DR，也可能同时是另一个网段的 BDR，还可能是第三个网段的 DROther。在图 8-2-8 中，路由器 R2 是 R1 和 R2 网段中的 BDR，是 R2 和 R3 网段中的

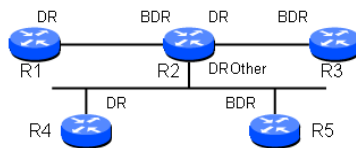


图 8-2-8 多重身份的路由器

DR，是 R2、R4 和 R5 网段中的 DROther。

8.2.8 OSPF 度量值计算*

在 8.2.6 节中，R1 可以学到 “O 3.3.3.3 [110/2] via 123.1.1.3, 00:26:35, FastEthernet0/0” 的 OSPF 路由，这里的度量值 2 是如何计算出来的呢？

OSPF 使用的度量值是 COST（花费）。在默认情况下，OSPF 以 100Mb/s 作为参考带宽，100Mb/s 除以实际链路的带宽，得出链路花费，从源到目标之间最短的链路花费被写入路由表。在前面配置的基础上，重新打开路由器 R3 的 Loopback 0 接口。在路由器 R3 上查看 Loopback 0 接口的带宽，显示如下：

```
R3#show interfaces loopback 0
Loopback0 is up, line protocol is up
Hardware is Loopback
Internet address is 3.3.3.3/24
MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
```

注意接口的带宽是 8000Mb/s，100Mb/s 除以 8000Mb/s，结果远小于 1，但度量值不能是 0，那就取最小的非零整数 1。在 R3 上验证 Loopback 0 接口的 OSPF 信息，显示如下：

```
R3#show ip ospf interface loopback 0
Loopback0 is up, line protocol is up
Internet Address 3.3.3.3/24, Area 0
Process ID 3, Router ID 33.3.3.3, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host
```

从上面的输出中，得出 R3 Loopback 0 链路的花费是 1，接下来看 R1 和 R3 之间以太网链路的花费。R1 和 R3 之间是快速的以太网，用 100Mb/s 除以 100Mb/s，结果是 1，1+1=2，R1 到 R3 Loopback 0 网段的花费是 2。接下来断开 R2 的快速以太网接口，并在 R2 上添加 Loopback 0 接口，IP 地址是 2.2.2.2/24，配置语句如下：

```
R2(config)#int loopback 0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
R2(config-if)#int fa 0/0
R2(config-if)#no shut
```

在路由器 R1 上查看 OSPF 的邻居，显示如下：

```
R1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
33.3.3.3	0	FULL/DROTHER	00:00:37	123.1.1.3	FastEthernet0/0
123.1.1.2	0	FULL/-	00:00:36	12.1.1.2	Serial1/1

从上面的输出中可以看到，R1 和 R2 之间只有一个邻接关系。“123.1.1.2”表示的是 Router ID，尽管路由器 R2 上的这个 IP 地址已经无效，且新配置了一个环回地址，可老的 Router ID 仍然有效，除非重启 OSPF 进程。R1 是 DR，R3 是 DROther，没有 BDR 的原因是 R3 的 Fa0/0 接口的 OSPF 优先级是 0，R3 不参与 DR 和 BDR 的选举。

查看 R1 的路由表，显示如下：

```
R1#show ip route
2.0.0.0/32 is subnetted, 1 subnets
O 2.2.2.2 [110/65] via 12.1.1.2, 00:06:35, Serial1/1
3.0.0.0/32 is subnetted, 1 subnets
O 3.3.3.3 [110/2] via 123.1.1.3, 00:06:35, FastEthernet0/0
123.0.0.0/24 is subnetted, 1 subnets
C 123.1.1.0 is directly connected, FastEthernet0/0
12.0.0.0/24 is subnetted, 1 subnets
C 12.1.1.0 is directly connected, Serial1/1
```

从上面的输出中可以看到, R1 从 R2 学到了 2.2.2.2/32 的主机路由, 度量值是 65。查看 R1 的 S1/1 接口的带宽是 1.544Mb/s, 100Mb/s 除以 1.544Mb/s, 结果约等于 64.7, 取整是 64, R1 和 R2 之间的链路花费是 64, 再加上 R2 环回接口的花费 1, 总共是 65。

auto-cost reference-bandwidth

从前面的叙述中读者可以发现, 在默认情况下, OSPF 使用 100Mb/s 作为参考带宽, 是无法区分出 100Mb/s、1000Mb/s 和 10000Mb/s 链路的, 因为它们的花费都是 1。

若要区分 100Mb/s、1000Mb/s 和 10000Mb/s 链路, 可以使用 10000Mb/s 作为参考带宽。使用的命令如下:

```
R1(config-router)#auto-cost reference-bandwidth 10000    把参考带宽改成 10000Mb/s。
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
```

上面的命令把 R1 的 OSPF 参考带宽改成了 10000Mb/s, 后面的提示说参考带宽已经被修改了, 请确保在所有的路由器上参考带宽的一致性。也就是说, 为了保证计量单位的一致性, 要把所有路由器的参考带宽都改成一致, 即都使用 10000Mb/s 作为参考带宽。使用同样的命令, 修改 R2 和 R3 的参考带宽。修改完成后, 再次查看 R1 的路由表, 显示如下:

```
R1#show ip route
 2.0.0.0/32 is subnetted, 1 subnets
O    2.2.2.2 [110/6477] via 12.1.1.2, 00:03:54, Serial1/1
 3.0.0.0/32 is subnetted, 1 subnets
O    3.3.3.3 [110/101] via 123.1.1.3, 00:03:54, FastEthernet0/0
123.0.0.0/24 is subnetted, 1 subnets
C    123.1.1.0 is directly connected, FastEthernet0/0
12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/1
```

$10000/8000=1.25$, 取整后是 1, $10000/1.544 \approx 6476.6$, 取整后是 6476, R1 去往 2.2.2.2/32 的度量值是 $6476+1=6477$ 。 $10000/100=100$, $10000/8000=1.25$, 取整后是 1, R1 去往 3.3.3.3/32 的度量值是 $100+1=101$ 。



8.3 OSPF 高级配置**

本节介绍 OSPF 验证和 OSPF 默认路由, 并演示 RIP 和 OSPF 共存的现象, 最后介绍 OSPF 故障排除技术。

8.3.1 OSPF 验证*

路由器能够设定密码来控制路由信息传播。在默认情况下, 路由器使用空验证, 也就是说, 进行路由信息交换是不验证的。继续使用图 8-2-5 中的配置, 在路由器 R1 上使用“debug ip ospf packet”命令检查 OSPF 数据分组的接收情况, 部分消息显示如下:

```
R1#debug ip ospf packet
OSPF packet debugging is on
R1#
*Mar 1 00:04:06.599: OSPF: rcv. v:2 t:1 l:52 rid:33.3.3.3
aid:0.0.0.0 chk:D884 aut:0 auk: from FastEthernet0/0
```

从上面的消息中可以看到, R1 收到了一个 OSPF 报文, “v:2”表示 OSPFv2; “t:1”表示 type=1, 类型 1 的报文是 Hello 报文; “l:52”表示 length=52, 即报文的长度是 52; “rid:33.3.3.3”表示发送路由器的 Router ID 是 33.3.3.3, 是从 R3 发过来的报文; “aid:0.0.0.0”表示所处的区域是 Area 0; “chk:D884”表示检验和; “aut:0”表示验证的类型是 0, 即没

有验证，验证类型为 1 表示明文验证，验证类型为 2 表示 MD5 验证；“auk”表示相关验证的内容；“from FastEthernet0/0”表示从哪一个接口接收 OSPF 报文。

OSPF 网络的验证有两种：简单明文验证（Simple Password Authentication）和 MD5 验证（Message Digest Authentication）。验证又可以分为针对链路的验证和针对区域的验证。针对链路的验证和 RIP、EIGRP 的类似，仅针对某一条链路。针对区域的验证是针对同一个 OSPF 区域中的所有路由器，要想参与 OSPF 路由，所有的路由器要配置相同的密码。本书中仅介绍 OSPF 的区域验证，更多的验证知识介绍属于 CCNP 部分的内容。

1. 简单明文验证

简单明文验证的缺点是易受攻击，任何人用线路分析仪都能从网络上窃取密码。在路由器 R1 上使用下面的命令启动简单明文验证：

```
R1(config)#int s1/1
R1(config-if)#ip ospf authentication-key cisco      在所有参与 OSPF 进程的接口上配置使用明文密码。

R1(config-if)#int fa 0/0
R1(config-if)#ip ospf authentication-key cisco
R1(config-if)#router ospf 1
R1(config-router)#area 0 authentication            声明 Area 0 使用明文验证。
```

配置完路由器 R1 后，暂不配置路由器 R2 和 R3，稍后 R1 上出现下面的消息：

```
*Mar 1 00:32:06.631: %OSPF-5-ADJCHG: Process 1, Nbr 33.3.3.3 on FastEthernet0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
*Mar 1 00:32:07.199: %OSPF-5-ADJCHG: Process 1, Nbr 123.1.1.2 on FastEthernet0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
*Mar 1 00:32:08.095: %OSPF-5-ADJCHG: Process 1, Nbr 123.1.1.2 on Serial1/1 from FULL to DOWN, Neighbor Down: Dead timer expired
```

提示所有的邻居都超时，邻居关系 Down 掉。使用“show ip ospf neighbor”命令查看 R1 的 OSPF 邻居，发现不了任何的邻居路由器。在路由器 R1、R2 或 R3 上使用“debug ip ospf adj”命令，调试 OSPF 的邻接关系，显示如下：

```
R1#debug ip ospf adj
OSPF adjacency events debugging is on
R1#
*Mar 1 00:44:46.675: OSPF: Rcv pkt from 123.1.1.3, FastEthernet0/0 : Mismatch
Authentication type. Input packet specified type 0, we use type 1
```

从上面的输出中可以看到，R1 从 Fa 0/0 接口收到 OSPF 报文，但验证类型不一致。进来的报文使用的验证类型是 0，即不采用验证；本路由器采用的验证类型是 1，即明文验证。验证类型不一致，邻接关系无法建立，更不可能交互路由信息了。继续使用下面的命令，配置路由器 R2 和 R3 使用明文验证：

```
R2(config)#int s1/0
R2(config-if)#ip ospf authentication-key cisco
R2(config-if)#int fa 0/0
R2(config-if)#ip ospf authentication-key cisco
R2(config-if)#router ospf 1
R2(config-router)#area 0 authentication
```

```
R3(config)#int fa 0/0
R3(config-if)#ip ospf authentication-key cisco
R3(config-if)#router ospf 3
R3(config-router)#area 0 authentication
```

配置完成后，R1、R2 和 R3 的邻接关系恢复正常，路由也可正常交互了。

2. MD5 验证

MD5 采用加密验证，每个路由器上都必须配置密码和密码 ID。路由器使用一种算法，基于 OSPF 报文、密码和密码 ID 产生一个 Hash（哈希）值，Hash 算法不可逆，用户很难从 Hash 值推导出密钥，然后把 Hash 值加到 OSPF 报文中。不像简单密码验证，MD5 验证时密码并不在网络上传输，传输的只是一个 Hash 值。每个 OSPF 报文中还包含一个序列号以保护网络不受攻击。

MD5 验证还有一个好处是可以更改密码而不中断网络业务，这有助于网络管理员在线更改 OSPF 验证密码。如果一个端口配置了一个新的密码，路由器将会向网络发送同一个报文的多个拷贝，每个报文用不同的密码来验证。当路由器检测到所有的邻居都采纳了新的密码后，就会停止发送老的密码报文。在路由器 R1 上使用下面的命令启动 MD5 验证：

```
R1(config)#int s1/1
R1(config-if)#no ip ospf authentication-key          取消之前的明文密码。
R1(config-if)#ip ospf message-digest-key 1 md5 cisco 配置 MD5 的密码和密码 ID。
R1(config-if)#int fa 0/0
R1(config-if)#no ip ospf authentication-key
R1(config-if)#ip ospf message-digest-key 1 md5 cisco
R1(config-if)#router ospf 1
R1(config-router)#area 0 authentication message-digest 区域 0 使用 MD5 验证。
```

R2 的配置如下：

```
R2(config)#int s1/0
R2(config-if)#no ip ospf authentication-key
R2(config-if)#ip ospf message-digest-key 1 md5 cisco
R2(config-if)#int fa 0/0
R2(config-if)#no ip ospf authentication-key
R2(config-if)#ip ospf message-digest-key 1 md5 cisco
R2(config-if)#router ospf 1
R2(config-router)#area 0 authentication message-digest
```

R3 的配置如下：

```
R3(config)#int fa 0/0
R3(config-if)#no ip ospf authentication-key
R3(config-if)#ip ospf message-digest-key 1 md5 cisco
R3(config-if)#router ospf 1
R3(config-router)#area 0 authentication message-digest
```

配置完成后，R1、R2 和 R3 的邻接关系恢复正常，路由也可正常交互了。

！ 注意：在配置路由器密码时，IOS 忽略密码前的空格，密码后的空格却被计算在内，在输入密码时要尤其当心，否则排查起来非常困难。

8.3.2 OSPF 默认路由***

在图 8-2-5 中，假设 R1 通过 ISP 连接到 Internet，如图 8-3-1 所示。路由器 R1 上配置了去往 Internet 的默认路由，可以使用“default-information originate”命令，向域内的其他 OSPF 路由器也发布默认路由。

这里给 R1 配置一个环回接口，假设该接口就是去往 ISP 的接口。配置命令如下：

```
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
```

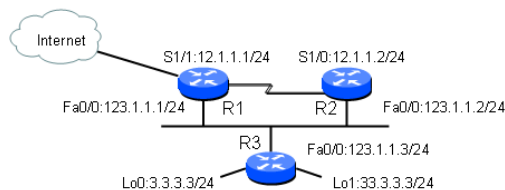


图 8-3-1 OSPF 默认路由

配置“default-information originate”命令，路由器 R1 向其他 OSPF 路由器发布一条默认路由。配置命令如下：

```
R1(config)#router ospf 1
R1(config-router)#default-information originate
```

配置完成后，查看 R2 的路由表，显示如下：

```
R2#show ip route
3.0.0.0/32 is subnetted, 1 subnets
O    3.3.3.3 [110/2] via 123.1.1.3, 00:07:14, FastEthernet0/0
123.0.0.0/24 is subnetted, 1 subnets
C    123.1.1.0 is directly connected, FastEthernet0/0
12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/0
O*E2 0.0.0.0/0 [110/1] via 123.1.1.1, 00:07:14, FastEthernet0/0
```

在 R2 的路由表中，可以看到“O*E2 0.0.0.0/0 [110/1] via 123.1.1.1, 00:07:14, FastEthernet0/0”，“O*”表示是通过 OSPF 学来的默认路由；“E2”表示该路由是 OSPF 外部类型 2 的路由，EIGRP 使用“EX”标记外部路由，OSPF 使用“E1”和“E2”来标记外部路由。“E1”表示外部类型 1 的路由，除了计算从外部进来的花费，还要算上 OSPF 域内的花费。“E2”表示外部类型 2 的路由，不再计算 OSPF 域内的花费，相比之下“E1”的度量值较大，但更准确。有关外部路由的更多知识属于 CCNP 部分的内容。

关闭路由器 R1 的 Loopback 0 接口，R2 和 R3 的路由表会出现什么变化呢？结果发现 R2 和 R3 的那条 OSPF 的默认路由消失了。仅当 R1 上有默认路由时，“default-information originate”命令才会影响 R1 向外发布默认路由，如果 R1 上的默认路由消失，该命令将不再向外发布默认路由。带 always 参数的“default-information originate”命令向外发布默认路由，而不管路由器本地有无默认路由。配置命令如下：

```
R1(config)#router ospf 1
R1(config-router)#default-information originate always
```

在 R1 环回接口关闭的情况下，带 always 参数的“default-information originate”命令使 R1 始终向外发布默认路由，而不管本地路由表中有没有默认路由。

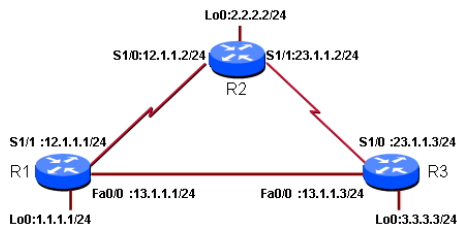


图 8-3-2 路由拓扑

R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#no cdp run
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int fa 0/0
R1(config-if)#ip add 13.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int lo0
```

8.3.3 RIP 升级到 OSPF**

这里介绍从 RIP 升级到 OSPF 的实验配置，从中读者可以了解到 OSPF 的快速收敛，OSPF 基于花费的度量值比 RIP 基于跳数的度量值更符合常理，OSPF 比 RIP 有更小的管理距离，路由选路原则的应用等知识点。

使用 RIPv1 配置如图 8-3-2 所示的网络拓扑。

```
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config-if)#router rip
R1(config-router)#net 1.0.0.0
R1(config-router)#net 12.0.0.0
R1(config-router)#net 13.0.0.0
```

R2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int lo0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
R2(config-if)#router rip
R2(config-router)#net 2.0.0.0
R2(config-router)#net 12.0.0.0
R2(config-router)#net 23.0.0.0
```

R3 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#no cdp run
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int fa 0/0
R3(config-if)#ip add 13.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
R3(config-if)#router rip
R3(config-router)#net 3.0.0.0
R3(config-router)#net 23.0.0.0
R3(config-router)#net 13.0.0.0
```

配置完成后, R1 的路由表显示如下:

```
R1#show ip route
 1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, Loopback0
R    2.0.0.0/8 [120/1] via 12.1.1.2, 00:00:13, Serial1/1
R    3.0.0.0/8 [120/1] via 13.1.1.3, 00:00:05, FastEthernet0/0
R    23.0.0.0/8 [120/1] via 13.1.1.3, 00:00:05, FastEthernet0/0
        [120/1] via 12.1.1.2, 00:00:13, Serial1/1
12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/1
13.0.0.0/24 is subnetted, 1 subnets
C    13.1.1.0 is directly connected, FastEthernet0/0
```

从上面的路由表中,可以得出两点结论:一是采用了自动汇总,R1 从 R2 和 R3 学到的是 2.0.0.0/8、3.0.0.0/8、23.0.0.0/8 路由,都被自动汇总了;二是 RIP 只是简单地根据跳数来判断路由的优劣,RIP 认为 R1 有两条去往 23.0.0.0/8 网段的等值路由,尽管一条是 100Mb/s,一条是 1.544Mb/s,而 RIP 考虑的仅是跳数,不符合常理。

在路由器 R1、R2 和 R3 上使用“no auto-summary”命令关闭自动路由汇总。

```
R1(config)#router rip
R1(config-router)#no auto-summary
```

```
R2(config)#router rip
R2(config-router)#no auto-summary
```

```
R3(config)#router rip
R3(config-router)#no auto-summary
```

再次查看 R1 的路由表，显示如下：

```
R1(config-router)#do show ip route
 1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, Loopback0
R    2.0.0.0/8 [120/1] via 12.1.1.2, 00:00:17, Serial1/1
R    3.0.0.0/8 [120/1] via 13.1.1.3, 00:00:07, FastEthernet0/0
R    23.0.0.0/8 [120/1] via 13.1.1.3, 00:00:07, FastEthernet0/0
      [120/1] via 12.1.1.2, 00:00:17, Serial1/1
 12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/1
 13.0.0.0/24 is subnetted, 1 subnets
C    13.1.1.0 is directly connected, FastEthernet0/0
```

从上面的输出中，发现 R1 的路由表并没有发生变化，在 RIPv1 中自动汇总是关闭不了的。读者顺便再回忆一下，RIPv1 是一个有类路由协议，不支持 VLSM 和 CIDR。

使用下面的命令把 RIP 从版本 1 升级到版本 2：

```
R1(config)#router rip
R1(config-router)#version 2
```

在 R2 和 R3 上执行同样的命令，升级到 RIPv2。如果马上查看 R1 的路由表，可能会看到这样的路由表：

```
R1#show ip route
 1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    1.1.1.0/24 is directly connected, Loopback0
R    1.0.0.0/8 [120/3] via 13.1.1.3, 00:00:15, FastEthernet0/0
      [120/3] via 12.1.1.2, 00:00:26, Serial1/1
 2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R    2.2.2.0/24 [120/1] via 12.1.1.2, 00:00:26, Serial1/1
R    2.0.0.0/8 [120/11] via 13.1.1.3, 00:00:00, FastEthernet0/0
 3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R    3.3.3.0/24 [120/1] via 13.1.1.3, 00:00:15, FastEthernet0/0
R    3.0.0.0/8 [120/14] via 12.1.1.2, 00:00:02, Serial1/1
 23.0.0.0/24 is subnetted, 1 subnets
R    23.1.1.0 [120/1] via 13.1.1.3, 00:00:15, FastEthernet0/0
      [120/1] via 12.1.1.2, 00:00:26, Serial1/1
 12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.1.0/24 is directly connected, Serial1/1
R    12.0.0.0/8 [120/14] via 13.1.1.3, 00:00:02, FastEthernet0/0
 13.0.0.0/24 is subnetted, 1 subnets
C    13.1.1.0 is directly connected, FastEthernet0/0
```

上面的路由表中出现了一些奇怪的路由（黑体标出的部分），这是因为 RIP 路由协议还没有收敛。等一会儿，大概几分钟，然后再查看 RIP 的路由表，显示如下：

```
R1#show ip route
 1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, Loopback0
 2.0.0.0/24 is subnetted, 1 subnets
R    2.2.2.0 [120/1] via 12.1.1.2, 00:00:22, Serial1/1
 3.0.0.0/24 is subnetted, 1 subnets
R    3.3.3.0 [120/1] via 13.1.1.3, 00:00:12, FastEthernet0/0
 23.0.0.0/24 is subnetted, 1 subnets
R    23.1.1.0 [120/1] via 13.1.1.3, 00:00:12, FastEthernet0/0
      [120/1] via 12.1.1.2, 00:00:22, Serial1/1
 12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/1
 13.0.0.0/24 is subnetted, 1 subnets
```

```
C 13.1.1.0 is directly connected, FastEthernet0/0
```

此时 RIP 路由协议已经收敛。R1 的路由表中出现了 24 位的路由条目，从这里可以得出结论：RIPv2 可以关闭自动汇总。读者顺便再回忆一下，RIPv2 是一个无类路由协议，支持 VLSM 和 CIDR，能关闭自动汇总，支持手工汇总。但不管是 RIPv1 还是 RIPv2，都存在一个共同的弱点，那就是慢速收敛。

接下来，继续在 R1、R2 和 R3 上配置 OSPF 路由，不要清除已有的 RIP 配置。R1 的配置如下：

```
R1(config)#router ospf 1
R1(config-router)#net 0.0.0.0 0.0.0.0 area 0
```

在 R2 和 R3 上执行类似的配置。都配置完成后，稍等片刻，路由器会提示 R1 与 R2 和 R3 的邻接关系已建立。然后查看 R1 的路由表，显示如下：

```
R1#show ip route
 1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, Loopback0
 2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O    2.2.2.2/32 [110/65] via 12.1.1.2, 00:01:40, Serial1/1
R    2.2.2.0/24 [120/1] via 12.1.1.2, 00:00:03, Serial1/1
 3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O    3.3.3.3/32 [110/2] via 13.1.1.3, 00:01:40, FastEthernet0/0
R    3.3.3.0/24 [120/1] via 13.1.1.3, 00:00:15, FastEthernet0/0
23.0.0.0/24 is subnetted, 1 subnets
O    23.1.1.0 [110/65] via 13.1.1.3, 00:01:40, FastEthernet0/0
12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/1
13.0.0.0/24 is subnetted, 1 subnets
C    13.1.1.0 is directly connected, FastEthernet0/0
```

从上面的输出中，可以发现 R1 的路由表中有两条 RIP 路由、三条 OSPF 路由。R1 的路由表中为何出现这样的路由，是不是路由表中会同时存有 RIP 和 OSPF 学来的所有路由条目？回答是否定的，在配置 OSPF 之前，R1 上有三条 RIP 路由，如果互不影响，R1 上现在应该还是有三条 RIP 路由，可为何变成两条了呢？比较一下，发现少了“R 23.1.1.0/24”的路由。这是因为 R1 通过 RIP 学到了 23.1.1.0/24 的路由，通过 OSPF 也学到了 23.1.1.0/24 的路由，路由表中只保存最优的路由，同样是 23.1.1.0/24 的路由，管理距离小的路由（OSPF 的管理距离是 110）更可信，被放入路由表，管理距离大的 RIP 路由（RIP 的管理距离是 120）在路由表中不显示。读者此时不免要问，那为何还有两条 RIP 路由存在呢？仔细看一下，通过 OSPF，R1 学到 R2 的环回接口是 32 位的主机路由 2.2.2.2/32，而通过 RIPv2 学到的是 2.2.2.0/24，掩码长度不同，这是两条不同的路由，都被放入路由表。

这里问一下，如果 R1 要去往 2.2.2.2，R1 选择的是 OSPF 路由还是 RIP 路由？可能所有的读者都能答对，选择 OSPF 路由。为什么选择 OSPF 路由呢？可能有的读者会回答，因为 OSPF 有更小的管理距离。没错，OSPF 是有更小的管理距离，可这里选择 OSPF 路由的原因不是因为管理距离，而是因为子网掩码长度，OSPF 路由能匹配 32 位，而 RIP 只能匹配 24 位。读者此时不妨回忆一下选路原则：第一条，最长匹配优先；第二条，管理距离小优先；第三条，度量值小优先。如果问 R1 要去往 2.2.2.3，R1 选择的是 RIP 路由还是 OSPF 路由呢？此时选择的就 RIP 路由了，因为 OSPF 路由不匹配。

在 R1 上使用“ip ospf network point-to-point”命令改变 R1 环回接口的网络类型，命令如下：

```
R1(config)#int lo0
R1(config-if)#ip ospf network point-to-point
```

在 R2 和 R3 上执行同样的命令，改变环回接口的 OSPF 网络类型为点到点，这样就会显示环回接口真实的网络路由，也就是变成 24 位的路由。再次查看 R1 的路由表，显示如下：

```
R1#show ip route
 1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, Loopback0
 2.0.0.0/24 is subnetted, 1 subnets
O    2.2.2.0 [110/65] via 12.1.1.2, 00:00:02, Serial1/1
 3.0.0.0/24 is subnetted, 1 subnets
O    3.3.3.0 [110/2] via 13.1.1.3, 00:00:02, FastEthernet0/0
23.0.0.0/24 is subnetted, 1 subnets
O    23.1.1.0 [110/65] via 13.1.1.3, 00:00:02, FastEthernet0/0
12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/1
 13.0.0.0/24 is subnetted, 1 subnets
C    13.1.1.0 is directly connected, FastEthernet0/0
```

从上面的输出中看不到 RIP 路由了。因为改变环回接口的类型后，OSPF 环回接口的路由也变成 24 位了，和 RIP 学到的网络一样。路由表中只保存最优的路由，管理距离小的 OSPF 路由进入路由表，管理距离大的 RIP 路由没有进入路由表。

既然 OSPF 已经配置成功，RIP 就成了一个多余的路由协议了。在 R1 上使用下面的命令，取消 RIP 协议：

```
R1(config)#no router rip
```

类似地，在 R2 和 R3 上使用相同的命令取消 RIP 协议，此时网络中只有单一的 OSPF 路由协议了。接下来演示一下 OSPF 的快速收敛，使用命令关闭 R2 的环回接口，马上查看 R1 的路由表，最多几秒钟，R1 的路由表中就清除了 R2 环回接口的路由。使用命令再打开 R2 的环回接口，马上查看 R1 的路由表，最多几秒钟，R1 的路由表中就添加了 R2 环回接口的准确路由。从这里可以看出，OSPF 能够快速收敛。

8.3.4 OSPF 故障排除**

这里结合 OSPF，介绍故障排除技术。网络拓扑如图 8-3-3 所示，IP 地址分配如表 8-3-1 所示。

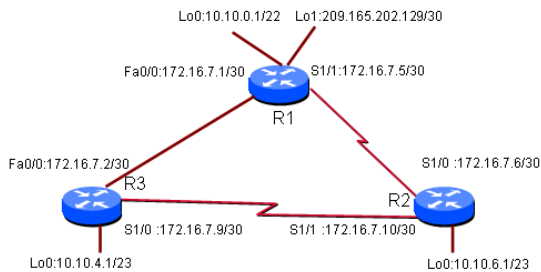


图 8-3-3 网络拓扑

表 8-3-1 IP地址分配

设 备	接 口	IP 地址	子网掩码
R1	Lo 0	10.10.0.1	255.255.252.0
	Lo 1	209.165.202.129	255.255.255.252
	S1/1	172.16.7.5	255.255.255.252
	Fa0/0	172.16.7.1	255.255.255.252

续表

设 备	接 口	IP 地址	子网掩码
R2	Lo 0	10.10.6.1	255.255.254.0
	S1/0	172.16.7.6	255.255.255.252
	S1/1	172.16.7.10	255.255.255.252
R3	Lo 0	10.10.4.1	255.255.254.0
	S1/0	172.16.7.9	255.255.255.252
	Fa0/0	172.16.7.2	255.255.255.252

学习目标

完成本实验，读者应该掌握下面的知识：

- 根据拓扑正确连接线缆。因为本实验中使用的是模拟器，线缆都已正确连接好。
- 删除启动配置文件，重新启动路由器，恢复路由器的出厂设置。
- 加载路由器预配置。
- 发现网络故障。
- 收集不正确的网络配置。
- 分析通信失败的原因。
- 找到可行性方案。
- 解决网络故障。
- 记录故障现象及处理结果。

场景

在这个实验中，读者要装入每台路由器的预配置。这些预配置中包含一些错误，读者需要找出预配置中的错误。当改正所有的错误后，所有路由器的环回接口间可以相互通信。每台路由器上都有一个环回接口用来模拟实际生产环境中的局域网接口。

读者改正配置时，要满足下面的要求：

- R1、R2 和 R3 都运行 OSPF 路由协议。
- 禁用所有路由器环回接口的更新，在实际环境中，局域网接口的路由更新也要禁用。
- R1 要把默认路由发布进 OSPF 域中的其他路由器。
- 所有 OSPF 路由器的 OSPF 进程号是 1。
- 所有 OSPF 路由器都工作在区域 0。

第一步：连线，删除路由器启动配置文件，重启路由器

① 连线

根据图中的拓扑进行连线。因为这里使用的是模拟机架，连线的工作就省去了。

② 清除每台路由器的配置

在实际的生产环境中，每台路由器上可能已经有启动配置文件了，需要删除已有的启动配置文件，然后重新启动路由器。因为这里使用的是模拟路由器，每台路由器配置寄存器的值都被设成了 0x2142，即启动时不加载启动配置文件（Startup-config），所以这个步骤也可以省去了。

```
Router#erase startup-config          删除路由器的启动配置文件。
Erasing the nvram filesystem will remove all configuration files! [Continfirm]
```

直接按回车键确认删除启动配置文件，按其他任意键放弃删除。

[OK]

Erase of nvram: complete

提示删除成功。

Router#reload

重新引导路由器。

System configuration has been modified. Save? [yes/no]: n

这里提示路由器的配置被修改了，是否要保存？这里要输入 no，不保存配置；如果输入 y，则是保存配置。如果保存了配置，再次启动时，路由器又有启动配置文件了，不会恢复出厂配置。

Proceed with reload? [confirm]

直接按回车键确认重启，按其他任意键放弃重启。

第二步：装入路由器的预配置

路由器重新启动后，在 “Would you like to enter the initial configuration dialog? [yes/no]:” 后输入 no，不进入初始配置对话框，然后输入 enable，configure terminal，进入路由器的全局配置模式，粘贴路由器的预配置。三台路由器的预配置文件在光盘中的 “配置\8\OSPF 排错” 文件夹下。R1 的部分配置如下：

```
hostname R1
no cdp run
no ip domain-lookup
interface loopback 0
ip address 10.10.10.1 255.255.252.0
ip ospf network point-to-point
no shutdown
interface loopback 1
ip address 209.165.202.129 255.255.255.252
no shutdown
interface fastethernet 0/0
ip address 172.16.7.1 255.255.255.252
no shutdown
interface s1/1
ip address 172.16.7.5 255.255.255.252
no shutdown
router ospf 1
log-adjacency-changes
passive-interface loopback 0
network 172.16.7.0 0.0.0.3 area 0
network 172.16.7.4 0.0.0.3 area 0
network 10.10.0.0 0.0.7.255 area 0
ip classless
ip route 0.0.0.0 0.0.0.0 loopback1
```

R2 的部分配置如下：

```
host R2
interface loopback 0
ip address 10.10.6.1 255.255.254.0
ip ospf network point-to-point
no shutdown
interface Serial1/1
ip address 172.16.7.10 255.255.255.252
no shutdown
interface Serial1/0
ip address 172.16.7.6 255.255.255.252
router ospf 1
log-adjacency-changes
passive-interface Serial1/0
network 172.16.7.4 0.0.0.3 area 0
network 172.16.7.8 0.0.0.3 area 0
network 10.10.6.0 0.0.1.255 area 0
ip classless
```

R3 的部分配置如下：

```
hostname R3
no cdp run
no ip domain-lookup
```

```

interface loopback 0
ip address 10.10.4.1 255.255.254.0
ip ospf network point-to-point
no shutdown
interface fastethernet 0/0
ip address 172.16.7.2 255.255.255.252
no shutdown
interface Serial1/0
ip address 172.16.7.9 255.255.255.252
no shutdown
router ospf 2
passive-interface Loopback 0
network 10.10.4.0 0.0.1.255 area 0
network 172.16.7.0 0.0.0.3 area 0
network 172.16.7.8 0.0.0.3 area 0
ip classless

```

第三步：排除物理层的故障

再次检查各路由器的连线是否正常。因为这里使用的是 Dynamips 模拟器，连线都是预配置的，均正常。如果是在真实环境或 Packet Tracer 模拟器中，还需要检查线缆类型，所连接的接口是否正确。

第四步：排除数据链路层的故障

① 检查路由器的串行接口有没有正确配置时钟参数。因为这里使用的是模拟器，不需要配置时钟，实际环境中或考试时要检查有没有配置时钟。

② 检查串行线路两端的封装协议是否一致。到目前为止，还没有介绍过串行接口的封装协议，串行接口默认使用的都是 HDLC 封装。广域网部分会介绍到串行接口的封装协议。

第五步：排除网络层接口的故障

检查路由器各接口的 IP 地址、子网掩码、端口状态是否正常。

① 在路由器 R1 上执行 “show ip int brief” 命令，显示如下：

```

R1#show ip int brief
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          172.16.7.1      YES manual up          up
Serial1/0                 unassigned      YES unset   administratively down down
Serial1/1                 172.16.7.5      YES manual up          down
Serial1/2                 unassigned      YES unset   administratively down down
Serial1/3                 unassigned      YES unset   administratively down down
FastEthernet2/0           unassigned      YES unset   administratively down down
Loopback0                 10.10.10.1      YES manual up          up
Loopback1                 209.165.202.129 YES manual up          up

```

从上面的输出中，可以发现路由器 Fa0/0 和 Lo1 接口的 IP 地址及状态均正常，Lo0 接口的 IP 地址配置错误，S1/1 接口硬件正常，但协议错误。使用 “show running-config” 命令进一步查看接口的子网掩码和接口下有没有别的无关配置。经检查路由器接口的子网掩码配置都正确，接口下也没有多余的配置。环回接口下的 “ip ospf network point-to-point” 命令是为了取消 32 位的主机路由。

更改路由器 R1 Lo0 接口的 IP 地址为 10.10.0.1。前面之所以配置成 10.10.10.1，多数是因为管理配置时输入有错。在 R1 上 ping R2 和 R3 的直连接口 IP 地址，发现 R3 正常，R2 失败，失败的原因很可能出现在 R2 上。

② 在路由器 R2 上执行 “show ip int brief” 命令，显示如下：

```

R2#show ip int brief
Interface                IP-Address      OK? Method Status      Protocol

```

FastEthernet0/0	unassigned	YES	unset	administratively	down	down
Serial1/0	172.16.7.6	YES	manual	administratively	down	down
Serial1/1	172.16.7.10	YES	manual	up	up	
Serial1/2	unassigned	YES	unset	administratively	down	down
Serial1/3	unassigned	YES	unset	administratively	down	down
FastEthernet2/0	unassigned	YES	unset	administratively	down	down
Loopback0	10.10.6.1	YES	manual	up	up	

从上面的输出中，可以发现路由器 R2 的 S1/0 接口状态是 administratively down，这是因为管理员没有使用“no shutdown”命令激活接口。打开路由器 R2 的 S1/0 接口，使用“show running-config”命令进一步查看接口的子网掩码和接口下有没有别的无关配置，发现均正常。

在 R2 上可以成功 ping 通 R1 和 R3 的直连接口。这里排除了 R1 不能 ping 通 R2 直连接口的故障。

③ 在路由器 R3 上查看接口 IP 地址、子网掩码、接口状态均正常，接口下也没有多余的配置。在 R3 上可以成功 ping 通 R1 和 R2 的直连接口。

第六步：排除网络层路由协议的故障

使用“show ip protocols”命令、“show ip ospf neighbor”命令查看各路由器路由协议的配置情况，使用“show ip route”命令查看各路由器路由表是否正确。一般的读者可能更喜欢使用“show running-config”命令，直接查看所有的配置。

① 在路由器 R1 上使用“show ip protocols”命令，显示如下：

```
R1#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.165.202.129
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.0.0 0.0.7.255 area 0
    172.16.7.0 0.0.0.3 area 0
    172.16.7.4 0.0.0.3 area 0
  Reference bandwidth unit is 100 mbps
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.4.1        110           00:09:32
    10.10.6.1        110           00:09:32
  Distance: (default is 110)
```

从上面的配置中，可以看出 OSPF 协议的进程号、参与 OSPF 协议的网络、被动接口的配置等。“10.10.0.0 0.0.7.255 area 0”这个网络的配置有误，路由器 R1 环回接口 Lo0 的 IP 地址是 10.10.0.1/22，正确的格式应该是“10.10.0.0 0.0.3.255”，使用下面的命令改正这个问题。

```
R1(config)#router ospf 1
R1(config-router)#no network 10.10.0.0 0.0.7.255 area 0
R1(config-router)#net 10.10.0.0 0.0.3.255 area 0
```

上面的不正确宣告，对于本实验来说，没有不正确影响，但如果路由器 R1 还有一个接口的 IP 地址范围在 10.10.4.0~10.10.7.255 区间，而该接口又没有运行 OSPF 协议，这样宣告的地址范围就会带来错误的影响。

使用“show ip ospf neighbor”命令查看路由器 R1 的 OSPF 邻居，显示如下：

```
R1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.10.4.1	1	FULL/BDR	00:00:34	172.16.7.2	FastEthernet0/0

从上面的输出中，可以发现 R1 只有一个 OSPF 邻居，与实际不符。少了一个邻居 R2，确认 R1 的配置没有错误，可能的错误出现在路由器 R2 上。

使用“show ip route”命令查看 R1 的路由表，显示如下：

```
R1#show ip route
172.16.0.0/30 is subnetted, 3 subnets
O    172.16.7.8 [110/65] via 172.16.7.2, 00:22:05, FastEthernet0/0
C    172.16.7.0 is directly connected, FastEthernet0/0
C    172.16.7.4 is directly connected, Serial1/1
209.165.202.0/30 is subnetted, 1 subnets
C    209.165.202.128 is directly connected, Loopback1
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O    10.10.4.0/23 [110/2] via 172.16.7.2, 00:22:05, FastEthernet0/0
O    10.10.6.0/23 [110/66] via 172.16.7.2, 00:22:05, FastEthernet0/0
C    10.10.0.0/22 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, Loopback1
```

R1 虽然学到了整个网络中的所有路由，但还是有缺陷的，因为 R1 和 R2 之间的 OSPF 邻接关系失败，R1 上的远程网络都是从 R3 学过来的。很显然，R1 去往 R2 上环回接口的路由应该是从 R2 直接过来更近。

② 在路由器 R2 上使用“show ip protocols”命令，显示如下：

```
R2#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.10.6.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.6.0 0.0.1.255 area 0
    172.16.7.4 0.0.0.3 area 0
    172.16.7.8 0.0.0.3 area 0
  Reference bandwidth unit is 100 mbps
  Passive Interface(s):
    Serial1/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.4.1        110          00:25:46
    209.165.202.129 110          00:25:46
  Distance: (default is 110)
```

从上面的配置中，可以看出 OSPF 协议的进程号、参与 OSPF 协议的网络、被动接口的配置等。“Serial1/0”这个接口是与 R1 相连的接口，需要建立 OSPF 邻接，发送路由更新的网络互连接口，不可能被配置成被动接口。R2 的环回接口不需要发送路由更新，需要设成被动接口。使用下面的命令改正这个问题：

```
R2(config)#router ospf 1
R2(config-router)#no passive-interface s1/0
R2(config-router)#passive-interface loopback 0
```

使用“show ip ospf neighbor”命令查看路由器 R2 的 OSPF 邻居，显示如下：

```
R2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.10.10.1	0	FULL/ -	00:00:32	172.16.7.5	Serial1/0
10.10.4.1	0	FULL/ -	00:00:36	172.16.7.9	Serial1/1

从上面的输出中，可以发现 R2 有两个 OSPF 邻居，关系都达到完全邻接状态。这里也排除了 R1 和 R2 之间邻接关系失败的故障。

使用“show ip route”命令，查看 R2 的路由表，显示如下：

```
R2#show ip route
  172.16.0.0/30 is subnetted, 3 subnets
C    172.16.7.8 is directly connected, Serial1/1
O    172.16.7.0 [110/65] via 172.16.7.9, 00:00:02, Serial1/1
    [110/65] via 172.16.7.5, 00:00:02, Serial1/0
C    172.16.7.4 is directly connected, Serial1/0
  10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O    10.10.0.0/22 [110/65] via 172.16.7.5, 00:00:02, Serial1/0
O    10.10.4.0/23 [110/65] via 172.16.7.9, 00:00:02, Serial1/1
C    10.10.6.0/23 is directly connected, Loopback0
```

从上面的输出中，R2 学到了整个 OSPF 域中的路由，可却没有去往 Internet 的默认路由。这是因为 R1 没有把自己上面的默认路由通告到 OSPF 域中。使用如下命令更改路由器 R1 的配置：

```
R1(config)#router ospf 1
R1(config-router)#default-information originate
```

再次查看 R2 的路由表，显示如下：

```
R2#show ip route
  172.16.0.0/30 is subnetted, 3 subnets
C    172.16.7.8 is directly connected, Serial1/1
O    172.16.7.0 [110/65] via 172.16.7.9, 00:00:27, Serial1/1
    [110/65] via 172.16.7.5, 00:00:27, Serial1/0
C    172.16.7.4 is directly connected, Serial1/0
  10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O    10.10.0.0/22 [110/65] via 172.16.7.5, 00:00:27, Serial1/0
O    10.10.4.0/23 [110/65] via 172.16.7.9, 00:00:27, Serial1/1
C    10.10.6.0/23 is directly connected, Loopback0
O*E2 0.0.0.0/0 [110/1] via 172.16.7.5, 00:00:27, Serial1/0
```

至此，R2 的路由表显示正确。

③ 在路由器 R3 上使用“show ip protocols”命令，显示如下：

```
R3#show ip protocols
Routing Protocol is "ospf 2"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.10.4.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.4.0 0.0.1.255 area 0
    172.16.7.0 0.0.0.3 area 0
    172.16.7.8 0.0.0.3 area 0
  Reference bandwidth unit is 100 mbps
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.6.1        110          00:25:46
  Distance: (default is 110)
```

从上面的输出中，可以看到运行的路由协议是 OSPF，但 OSPF 进程号是 2。在 OSPF 的配置中，进程号只具有本地意义，不影响全局配置，但题目中明确要求，所有路由器的 OSPF 进程号要配置成 1。

从上面的输出中，可以看到三个网段和区域宣告也是正确的；环回接口也被配成了被动接口，不对外发送路由更新。使用下面的命令更改路由器 R3 的配置：

```
R3(config)#no router ospf 2
R3(config)#router ospf 1
R3(config-router)#passive-interface Loopback0
R3(config-router)#network 10.10.4.0 0.0.1.255 area 0
R3(config-router)#network 172.16.7.0 0.0.0.3 area 0
```

```
R3(config-router)#network 172.16.7.8 0.0.0.3 area 0
```

使用“show ip ospf neighbor”命令查看路由器 R3 的 OSPF 邻居，显示如下：

```
R3#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.10.6.1	0	FULL/ -	00:00:38	172.16.7.10	Serial1/0
209.165.202.129	1	FULL/DR	00:00:39	172.16.7.1	FastEthernet0/0

从上面的输出中，可以发现 R3 有两个 OSPF 邻居，关系都达到完全邻接状态。

使用“show ip route”命令，查看 R3 的路由表，显示如下：

```
R3#show ip route
 172.16.0.0/30 is subnetted, 3 subnets
C    172.16.7.8 is directly connected, Serial1/0
C    172.16.7.0 is directly connected, FastEthernet0/0
O    172.16.7.4 [110/65] via 172.16.7.1, 00:04:40, FastEthernet0/0
 10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O    10.10.0.0/22 [110/2] via 172.16.7.1, 00:04:40, FastEthernet0/0
C    10.10.4.0/23 is directly connected, Loopback0
O    10.10.6.0/23 [110/65] via 172.16.7.10, 00:04:40, Serial1/0
O*E2 0.0.0.0/0 [110/1] via 172.16.7.1, 00:04:40, FastEthernet0/0
```

从上面的输出中，可以看出 R3 学到了整个 OSPF 域中的路由，包括外部路由。路由表完全正常。

第七步：测试

在 R1 上测试 Lo0 口到 R2 上 Lo0 口网络的连通性。测试如下：

```
R1#ping
Protocol [ip]:
Target IP address: 10.10.4.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.10.0.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.4.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.0.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/32/44 ms
```

从上面的输出中，可以看出 R1 的环回接口可以成功 ping 通 R3 的环回接口。

类似地，可以测试 R1 的环回接口到 R2 的环回接口，R2 的环回接口到 R3 的环回接口都可以 ping 通。R2 和 R3 也可以 ping 通 R1 的 Loopback 1 接口。至此，整个网络调试完成。

后面还会讲到访问控制列表，路由可达并不能保证 ping 包可达；ping 包可达，并不能保证 Telnet 可达，那时还需要对访问控制列表进行排错。

第八步：保存配置，记录文档

使用“write”或“copy run start”命令保存路由器 R1、R2 和 R3 的配置，并在文档中记录此次排错的步骤和心得，随着经验的不断积累，排错花费的时间会越来越短，排错的能力也会越来越强。



8.4 真题精选***

- On point-to-point networks, OSPF hello packets are addressed to which address?
 A. 127.0.0.1 B. 172.16.0.1 C. 192.168.0.5
 D. 223.0.0.1 E. 224.0.0.5 F. 254.255.255.255
- The OSPF Hello protocol performs which of the following tasks? (Choose two.)
 A. It provides dynamic neighbor discovery.
 B. It detects unreachable neighbors in 90 second intervals.
 C. It maintains neighbor relationships.
 D. It negotiates correctness parameters between neighboring interfaces.
 E. It uses timers to elect the router with the fastest links as the designated router.
 F. It broadcasts hello packets throughout the internetwork to discover all routers that are running OSPF.
- Which of the following describe the process identifier that is used to run OSPF on a router? (Choose two.)
 A. It is locally significant.
 B. It is globally significant.
 C. It is needed to identify a unique instance of an OSPF database.
 D. It is an optional parameter required only if multiple OSPF processes are running on the router.
 E. All routers in the same OSPF area must have the same process ID if they are to exchange routing information.
- Refer to the exhibit. A network associate has configured OSPF with the command:
 City(config-router)# network 192.168.12.64 0.0.0.63 area 0 After completing the configuration, the associate discovers that not all the interfaces are participating in OSPF. Which three of the interfaces shown in the exhibit will participate in OSPF according to this configuration statement? (Choose three.)

City#show ip interface brief						
Interface	IP-Address	OK?	Method	Status	Protocol	
FastEthernet0/0	192.168.12.48	YES	manual	up	up	
FastEthernet0/1	192.168.12.65	YES	manual	up	up	
Serial0/0	192.168.12.121	YES	manual	up	up	
Serial0/1	unassigned	YES	unset	up	up	
Serial0/1.102	192.168.12.125	YES	manual	up	up	
Serial0/1.103	192.168.12.129	YES	manual	up	up	
Serial0/1.104	192.168.12.133	YES	manual	up	up	
City#						

- FastEthernet0 /0 B. FastEthernet0 /1 C. Serial0/0
 D. Serial0/1.102 E. Serial0/1.103 F. Serial0/1.104
- Refer to the exhibit. Router1 was just successfully rebooted. Identify the current OSPF router ID for Router1.
 A. 190.172.32.10 B. 208.149.23.162
 C. 208.149.23.194 D. 220.173.149.10

```
Router1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	190.172.32.10	YES	NVRAM	up	up
Loopback0	208.149.23.162	YES	NVRAM	up	up
Loopback1	208.149.23.194	YES	NVRAM	up	up
Serial0	220.173.149.10	YES	manual	down	down
Serial1	unassigned	YES	NVRAM	administratively down	down

6. On which types of network will OSPF elect a backup designated router?

- A. point-to-point and multiaccess
- B. point-to-multipoint and multiaccess
- C. point-to-point and point-to-multipoint
- D. nonbroadcast and broadcast multipoint
- E. nonbroadcast and broadcast multiaccess

7. Refer to the exhibit. Why are two OSPF designated routers identified on Core_Router?

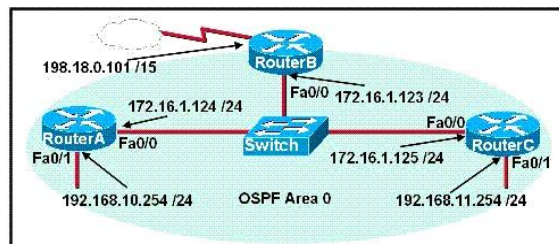
```
Core_Router# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
208.149.23.194	1	FULL/DR	00:00:33	190.172.32.10	Ethernet1
208.149.23.66	1	FULL/BDR	00:00:32	190.171.23.13	Ethernet0
208.149.23.130	1	FULL/DR	00:00:39	190.171.23.10	Ethernet0

```
Core_Router#
```

- A. Core_Router is connected to more than one multiaccess network.
- B. The router at 208.149.23.130 is a secondary DR in case the primary fails.
- C. Two router IDs have the same OSPF priority and are therefore tied for DR election.
- D. The DR election is still underway and there are two contenders for the role.

8. A network administrator is configuring the routers in the graphic for OSPF. The OSPF process has been started and the networks have been configured for Area 0 as shown in the diagram. The network administrator has several options for configuring RouterB to ensure that it will be preferred as the designated router (DR) for the 172.16.1.0 /24 LAN segment. What configuration tasks could be used to establish this preference? (Choose three.)



- A. Configure the priority value of the Fa0/0 interface of RouterB to a higher value than any other interface on the Ethernet network.
- B. Change the router id of Router B by assigning the IP address 172.16.1.130/24 to the Fa0/0 interface of RouterB.
- C. Configure a loopback interface on RouterB with an IP address higher than any IP address

on the other routers.

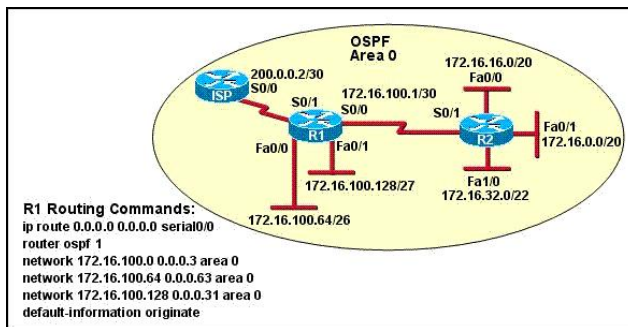
- D. Change the priority value of the Fa0/0 interface of RouterB to zero.
 - E. Change the priority values of the Fa0/0 interfaces of RouterA and RouterC to zero.
 - F. No further configuration is necessary.
9. Refer to the exhibit. Why was RouterA not elected as the designated router?

```
RouterA# show ip protocols
Routing Protocol is "ospf 109"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 221.130.149.10
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    190.171.23.0 0.0.0.255 area 0
    190.172.32.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    208.149.23.66    110           00:20:09
    208.149.23.194    110           00:20:09
    208.149.23.130    110           00:20:09
  Distance: (default is 110)

RouterA# show ip ospf interface
Ethernet1 is up, line protocol is up
  Internet Address 190.172.32.11/24, Area 0
  Process ID 109, Router ID 221.130.149.10, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State EDR, Priority 1
  Designated Router (ID) 208.149.23.194, Interface address 190.172.32.10
  Backup Designated router (ID) 221.130.149.10, Interface address 190.172.32.11
<output omitted>
```

- A. The interface address of RouterA is a higher value than the interface address of the DR.
- B. The OSPF process ID of RouterA is lower than the process ID of the elected DR.
- C. RouterA has a lower OSPF priority value than the router elected as DR.
- D. RouterA is not advertising the interface with address 221.130.149.10.

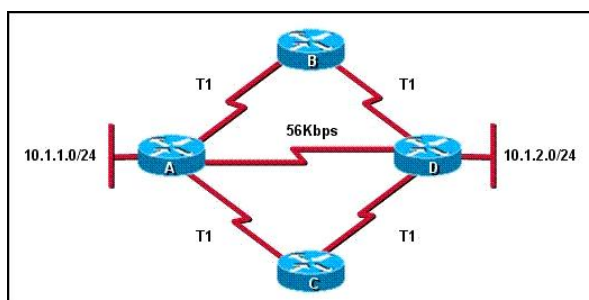
10. Refer to the exhibit. Assume that all router interfaces are operational and correctly configured. In addition, assume that OSPF has been correctly configured on router R2. How will the default route configured on R1 affect the operation of R2?



- A. Any packet destined for a network that is not directly connected to router R1 will be dropped.
- B. Any packet destined for a network that is not directly connected to router R2 will be dropped immediately.
- C. Any packet destined for a network that is not directly connected to router R2 will be dropped immediately because of the lack of a gateway on R1.
- D. The networks directly connected to router R2 will not be able to communicate with the 172.16.100.0, 172.16.100.128, and 172.16.100.64 subnetworks.

E. Any packet destined for a network that is not referenced in the routing table of router R2 will be directed to R1. R1 will then send that packet back to R2 and a routing loop will occur.

11. Refer to the exhibit. How will router A choose a path to the 10.1.2.0/24 network when different routing protocols are configured? (Choose three.)



- A. If RIPv2 is the routing protocol, only the path AD will be installed in the routing table by default.
- B. If RIPv2 is the routing protocol, the equal cost paths ABD and ACD will be installed in the routing table by default.
- C. If EIGRP is the routing protocol, only the path AD will be installed in the routing table by default.
- D. If EIGRP is the routing protocol, the equal cost paths ABD and ACD will be installed in the routing table by default.
- E. If EIGRP and OSPF are both running on the network, the EIGRP paths will be installed in the routing table.
- F. If EIGRP and OSPF are both running on the network, the OSPF paths will be installed in the routing table.

12. A routing protocol is required that supports:

- 1) routing update authentication
- 2) an addressing scheme that conserves IP addresses
- 3) multiple vendors
- 4) a network with over 50 routers

Which routing protocol fulfills these requirements?

- A. RIPv1
- B. RIPv2
- C. EIGRP
- D. OSPF

13. A network administrator is troubleshooting the OSPF configuration of routers R1 and R2. The routers cannot establish an adjacency relationship on their common Ethernet link. The graphic shows the output of the show ip ospf interface e0 command for routers R1 and R2. Based on the information in the graphic, what is the cause of this problem?

- A. The OSPF area is not configured properly.
- B. The priority on R1 should be set higher.
- C. The cost on R1 should be set higher.
- D. The hello and dead timers are not configured properly.
- E. A backup designated router needs to be added to the network.

F. The OSPF process ID numbers must match.

```

R1: Ethernet0 is up, line protocol is up
     Internet address 192.168.1.2/24, Area 0
     Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost: 10
     Transmit Delay is 1 sec, State DR, Priority 1
     Designated Router (ID) 192.168.31.33, Interface address 192.168.1.2
     No backup designated router on this network
     Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5

R2: Ethernet0 is up, line protocol is up
     Internet address 192.168.1.1/24, Area 0
     Process ID 2, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 10
     Transmit Delay is 1 sec, State DR, Priority 1
     Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1
     No backup designated router on this network
     Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

```



8.5 真题解答***

1. 解: E

题目问: 在点对点网络中, OSPF Hello 包发送的地址是多少? 在 OSPF 中 Hello 包发送的是 224.0.0.5 和 224.0.0.6 这两个地址。224.0.0.5 代表的是一般 OSPF 路由器, 224.0.0.6 代表的是多路访问网络中的 DR 和 BDR, 在点对点的网络中, 不需要选举 DR 和 BDR, Hello 包发送的地址是 224.0.0.5。

2. 解: AC

题目问: OSPF 中 Hello 包的作用是什么 (选两个)? OSPF 中 Hello 包的作用是发现和维持邻居关系。

3. 解: AC

题目问: 哪一句描述了 OSPF 路由器上的进程号标识 (选两个)? OSPF 的进程号仅在本路由器上有效, 路由器不同的接口可以配置在不同的区域内, 相邻路由器的接口要配置在同一个区域内, OSPF 对不同路由器上的 OSPF 进程号没有要求。但在同一台路由器上可以配置多个 OSPF 进程, 不同的 OSPF 进程使用不同的进程号, 路由器为每个进程维护各自的 OSPF 数据库, 两个 OSPF 数据库独立工作, 相互间不受影响, 但在实际工程中, 很少见到在同一台路由器上配置两个 OSPF 进程的情况。

4. 解: BCD

题目问: 参照图, 一个网络副手使用 “City(config-router)# network 192.168.12.64 0.0.0.63 area 0” 命令配置 OSPF, 配置完成后, 网络副手发现并不是所有的接口都参与了 OSPF, 那条配置语句使图中显示的哪三个接口参与了 OSPF? 192.168.12.64 0.0.0.63 匹配的地址范围是 192.168.12.64~192.168.12.127, IP 地址在此范围内的接口将参与 OSPF 进程, 所以被激活的接口有 FastEthernet0/1、Serial0/0、Serial0/1.102。

5. 解: C

题目问: 参照图, Router1 路由器刚刚重新启动, OSPF 的 Router ID 是多少? 这是一个关于 OSPF 的 RID 的选举的问题, 根据本章 8.2.7 节介绍的 Router ID 选举, 在 OSPF 中, RID 的选举过程是这样的: 如果通过命令 router-id 来指定一个 RID, 那么就采用手工指定的这个 RID; 如果没有手工指定, 则在可以使用的接口中来选举, 优先采用环回接口。如

果只有一个环回接口，就采用这个环回接口的 IP 地址作为 RID；如果有多个环回接口，就采用这多个环回接口中 IP 地址最大的作为 RID；如果没有环回接口，就采用物理接口中 IP 地址最大的接口 IP 地址作为 RID。值得注意的是，不管是环回接口还是物理接口，被使用 shutdown 命令关闭的接口要除外。在图中可以看到有两个环回接口，而 Loopback1 的 IP 地址更大，所以 208.149.23.194 就作为 RID 了。

6. 解：E

题目问：在什么样类型的网络中，OSPF 将选举 BDR？DR、BDR 的选举发生在多路访问的网络中，所谓多路访问的网络，就是指使用共享传输介质，同一个子网中可以存在多台路由器，比如以太网是支持广播的多路访问，帧中继是不支持广播的多路访问，点对点链路只有两个结点不属于多路访问网络。不管是否支持广播，多路访问的网络都需要选举 DR 和 BDR。

7. 解：A

题目问：参照图，在 Core_Router 路由器的邻居表中，为什么会出现两个 DR 路由器？本章的 8.2.7 节介绍了 DR 和 BDR 选举，DR 和 BDR 的选举是针对路由器所在的网段，而不是针对路由器本身进行的。某一台路由器对一个网段来说是 DR，对另一个网段来说可能是 BDR。Core_Router 路由器的 Ethernet0 和 Ethernet1 处在不同的多路访问网络中，两个网络都需要选举 DR 和 BDR。

8. 解：ACE

题目问：一个网络管理员配置图中的 OSPF 路由器，OSPF 进程已经开始，网络也被配置在区域 0 中，网络管理员有几种选择用来确保 RouterB 能成为 172.16.1.0/24 网段中的 DR，什么样的任务被用来完成这种配置（选三个）？OSPF 在共享介质下需要选举 DR 和 BDR，而这个选举的过程是通过比较优先级和 RID 来实现的。优先级越高的越有可能被选举成为 DR，优先级为 0 的接口不参加 DR 的选举，如果优先级相同就比较它们的 RID，RID 越大的越优先。RID 的选举过程在前面的考题中已经介绍过。考题中需要确保 RouterB 成为网络 172.16.1.0/24 的 DR，根据上面的解释可以看出，让它成为 DR 的方式有：更改 RouterB 的 Fa0/0 的优先级为最大的；更改 172.16.1.0/24 网段上的其他接口（也就是 RouterA 和 RouterC 的 Fa0/0 接口）的优先级为 0；设置 RouterB 的 RID 最大。又因为 OSPF 进程已经开始，网络中的 DR 和 BDR 已经选举出来了，即使修改了路由器的接口优先级或 RID，也不一定会引起 DR 和 BDR 的重新选举。为了让网络中能重新选举 DR 和 BDR，需要重新启动 RouterA 和 RouterC，或者使用“clear ip ospf process”命令来重新启动这两台路由器上的 OSPF 进程。综上所述，ACE 正确，F 选项说不需要进一步的配置是错误的，配置 ACE 中的步骤并不会引起 DR 的重新选举。

9. 解：C

题目问：根据输出，为什么 RouterA 没有被选举为 DR？从“show ip ospf interface”命令的输出中，可以看到 RouterA 的 RID 是 221.130.149.10，网络类型是广播型（需要选举 DR 和 BDR），在 190.172.32.0/24 网段，RouterA 是 BDR，接口的优先级是 1，DR 是 208.149.23.194，DR 在该网段接口的 IP 地址是 190.172.32.10。考虑 DR 的选举过程，首先考虑的是接口的优先级，假设两个接口的优先级一样，考虑的是 RID，RID 高的将被选举为 DR，RouterA 的 RID 是 221.130.149.10，高于 DR 的 RID 208.149.23.194，这说明假设错

误, DR 的接口优先级高于 RouterA 的接口优先级, 即 C 选项正确。A 选项说是因为 RouterA 在 190.172.32.0/24 网段的 IP 地址 190.172.32.11 高于 DR 的 IP 地址 190.172.32.10, 这是错误的, DR 的选举与 RID 有关, 与网段接口具体的 IP 地址无关; B 选项提到了 OSPF 的进程号, DR 的选举与 OSPF 进程号无关; D 选项说 RouterA 没有通告 IP 地址是 221.130.149.10 的接口, 从 “show ip protocols” 命令的输出中, 的确可以看到 RouterA 的 OSPF 进程中没有通告这个接口, 但一个接口有没有通告到 OSPF 进程中, 并不会影响这个接口的 IP 地址能否成为 RID, 也不会影响路由器能否成为 DR。特别值得一提的是, 很多题库中都错误地把 D 当成了正确的选项。

10. 解: E

题目问: 参照图, 假设所有路由器接口都正常并且被正确配置, 路由器 R2 也被正确配置了 OSPF, R1 的 OSPF 配置如图中所示, R1 上默认路由的配置将会怎样影响 R2 的操作? R1 上的 “ip route 0.0.0.0 0.0.0.0 serial0/0” 命令配置了一条默认路由, 默认路由的出口是 serial0/0, 其实这里是配置错误, 在现实的环境中, 默认路由的外出接口应该是 serial0/1。R1 上的 “default-information originate” 命令向 OSPF 域内的其他 OSPF 路由器发布一条默认路由, R2 上将会学到一条指向 R1 的 OSPF 默认路由。R2 收到任何路由表中没有的目的网段时, 就将数据包转发给 R1, 而 R1 也没有这样的路由, 根据默认路由的外出接口又将数据包转发给 R2, 这样就形成了一个路由的环路。

11. 解: ADE

题目问: 参照图, 当配置不同路由协议时, 路由器 A 将怎样选择去往 10.1.2.0/24 的路径 (选三个)? A 选项说, 当使用 RIPv2 路由协议时, 在默认情况下, 只有路径 AD 被放置到路由表中, 该选项是正确的, RIP 的度量值只有跳数, 跳数越小越优先; B 选项则是错误的; C 选项说, 如果使用的是 EIGRP, 在默认情况下只有 AD 被放置到路由表中, EIGRP 使用的度量值是带宽+延时。在默认情况下, 度量值的公式是: $(10000M/\text{链路上的最小带宽} + \text{延时总和}/10) * 256$, T1 是 1.544Mb/s 链路, T1 的延时应该小于 56Kb/s 的延时, 就算延时相等, 延时对度量值的影响远没有带宽产生的影响大, ABD 和 ACD 的链路度量值应小于 AD 链路的度量值, 故 C 选项错误; D 选项则正确; E 选项说, 如果 EIGRP 和 OSPF 同时被配置在网络上, EIGRP 的路由将被放置到路由表中, 根据路由选路原则, 对于相同的网络, 管理距离越小越优先, EIGRP 的管理距离是 90, OSPF 的管理距离是 110, EIGRP 优先, 故正确; F 选项错误。

12. 解: D

题目问: 一个路由协议要求支持下面的特性:

- (1) 路由更新支持认证;
- (2) 支持节省 IP 地址的架构 (这里要求的是支持 VLSM);
- (3) 支持多厂商;
- (4) 网络中超过 50 台路由器。

哪一个路由协议能满足这些要求? RIPv1 不支持认证, 也不支持 VLSM, 可以排除选项 A。EIGRP 是思科私有的, 不支持多厂商, 可以排除选项 C。网络的大小可以超过 50 台路由器, RIPv2 将很难胜任, 因为 RIP 最大只能支持 15 跳, 可以排除选项 B。最后只有选项

D, OSPF 可以满足要求。

13. 解: D

题目问: 一个网络管理员排除路由器 R1 和 R2 的 OSPF 配置故障。两台路由器在共同的以太网链路上不能建立邻接关系。图中给出了两台路由器上 “show ip ospf interface e0” 命令的输出, 基于图中的信息, 是什么原因导致了两台路由器的邻接关系不能建立? 参照本章的 8.2.4 节, 两台路由器要建立邻接关系, Hello 报文中的一些参数要匹配才可以, 这些参数包括: Hello time 和 Dead time、Area id、特殊区域标识符 (CCNA 中不涉及), 验证要通过。然后比较图中的 R1 和 R2 的内容, 可以看到它们的 Hello time 和 Dead time 是不同的, 因此它们的邻居关系无法建立。

第 9 章

交换机**

本章主要介绍思科的分层体系架构、交换机的分类和交换机的基本配置，重点介绍最常见的 ARP 攻击的原理、判断方法和解决办法。

9.1 局域网设计**

在商业化的今天，对中小企业来说，能够使数据、语音和视频通信数字化关系到企业的生死存亡。一个好的局域网离不开良好的设计和合适的网络设备。本节介绍思科的分层体系架构和相关原则，使读者能够选取合适的交换机设备。

9.1.1 分级网络设计**

如果使用分级（hierarchical）设计模型来建立一个局域网满足中小企业需求，则很容易成功。和其他网络设计相比，分等级的网络更容易管理和扩展，排除故障也迅速。

分级网络设计把一个复杂的网络问题分解为多个小的、更容易管理的问题，每一层（级）负责解决特定的问题。典型的分级设计模型把网络设计分成三层：接入层（Access）、汇聚层（Distribution）和核心层（Core）。

（1）接入层

接入层为终端设备（典型的如计算机、打印机、IP 电话等）提供访问接口。接入层也可以包括路由器、交换机、网桥、无线 AP 等设备。如图 9-1-1 所示，最下面部分就是接入层。一般在接入层实施冲突域的隔离、VLAN 的划分和交换机的端口安全。

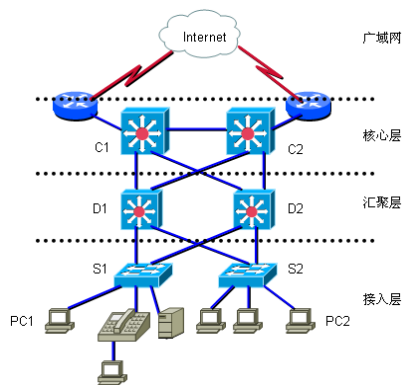


图 9-1-1 分层网络设计

（2）汇聚层

汇聚层位于接入层和核心层之间，它把核心层同网络的其他部分区分开来。该层的目的是实现 VLAN 间的通信和广播域的划分，并定义了网络的策略（Policy）。策略是控制某些类型通信的一种方法，这些通信类型包括路由更新、路由汇总、VLAN 间通信、地址聚合、访问控制和路由的重分布等。该层的位置如图 9-1-1 所示。

（3）核心层

核心层只有一个用途，那就是快速转发。在该层的设备不应该承担访问列表检查、数据加密、MAC 地址绑定、网络地址转换、路由汇聚或

其他影响数据快速交换的任务。该层的位置如图 9-1-1 所示。

1. 分级网络设计的优点

使用分级网络设计有很多优点，包括：

- **扩展性**。分级网络很容易被扩展。
- **冗余性**。如图 9-1-1 所示，在汇聚层和核心层提供冗余路径，确保路径可用。
- **高性能**。在图 9-1-1 中，可以把接入层上连至汇聚层、汇聚层上连至核心层的多条链路进行汇聚，以提供更高速的带宽。有关汇聚，属于 CCNP 的内容。
- **高安全性**。在接入层实施端口安全，在汇聚层实施策略，使一些不安全因素被限制在更小的范围内，不至于影响到核心层，这样网络变得更安全。
- **可管理性**。模块化的配置更加易于管理，当一台新交换机被加入网络中时，它的配置可以借鉴甚至是拷贝其他交换机的配置。
- **易维护性**。分级网络设计结构清晰，易于维护。

2. 分级网络设计的原则

一个网络分级并不意味着就是一个好的设计，衡量分级网络设计优劣可以从下面几个方面考虑。

(1) 网络直径 (Network Diameter)

网络直径是指从源设备到目标设备之间经过设备的数量。在图 9-1-1 中，假设从 PC1 到 PC2 要经过 S1—D1—C1—C2—D2—S2，网络的直径是 6。在路径上的每一台交换机都会产生延时，尽管每台交换机的延时很小，但很多交换机累积起来的延时可能很大。保持网络直径在一个小的范围，可以减小网络的延迟，并使网络的延迟可预测。

分级网络设计的第二层可以有效地减小网络直径。在图 9-1-1 中，假设 PC1 和 PC2 属于不同的部门，在汇聚层的 D1 设备上，可以实现 VLAN 间的通信，则 PC1 到 PC2 的路径是 S1—D1—S2，网络的直径是 3。

(2) 带宽聚合 (Bandwidth Aggregation)

在图 9-1-1 中，可以在 S1 和 D1 之间连接多条线缆，并配置链路聚合，以提供更快速的的上连链路，提供更高的吞吐量。

(3) 冗余 (Redundancy)

冗余是创建高可用网络的一部分。冗余分为链路冗余和设备冗余。在图 9-1-1 中，任何两台交换机间的链路故障都不会影响网络的正常通信，这使用的是链路冗余。除接入层 S1 和 S2，任何一台交换机的故障也不会影响网络的通信，这使用的是设备冗余。在一般的网络中，为了保障高可用性，往往是同时使用链路冗余和设备冗余。

一个企业使用什么样的网络，往往与企业的业务需求和财力有关。很多企业往往为了省钱或配置简单，使用的是平面型的网络，很多交换机杂乱无章地连在一起，经常是一台电脑中毒，全公司电脑中毒；部分网络瘫痪，全公司网络瘫痪。

说出来，读者可能不信，笔者曾遇到一个事业单位，接入层配置的都是思科 3560 交换机，通过交换机的级联，所有的部门都配置在同一个子网中。所有的三层交换机都是默认的出厂配置，当成普通的非网管二层交换机使用，在 ARP 病毒盛行的当今，每天网络至少有三分之一的时间是中断的。

9.1.2 交换机选型*

交换机和路由器一样，也分为固定配置和模块化交换机。此外有的交换机还支持堆叠，这又可分为可堆叠和不可堆叠交换机。

(1) 固定配置交换机

固定配置交换机使用固定的配置，不可添加或删除端口。例如，如果购买的是 24 口百兆交换机，交换机上配置了 24 个端口，就是 24 个端口，不可以扩展到 48 个端口，也不可以把百兆端口替换成千兆端口。

(2) 模块化交换机

模块化交换机提供更多的灵活性。模块化交换机通常配置了不同大小的机箱，以便安装不同的模块化线路卡。如果购买了模块化交换机，配备了 24 个端口模块，可以轻松添加额外的 24 个端口模块，使端口总数达到 48 个。

(3) 可堆叠交换机

可堆叠交换机可以使用一根背板电缆相互连接，在交换机间提供高的吞吐量，可以把堆叠的多台交换机当成一台交换机对待。多台交换机可以通过级联的方式连接在一起，也可以通过堆叠的方式连接在一起。图 9-1-2 中左边部分是交换机间的级联，右边是交换机间的堆叠。

级联是通过网络传输介质把多台相同的交换机连接起来。根据传输介质的不同，两台交换机间距离也不同，级联的速度要受传输介质的影响，传输介质的带宽一般是 100Mb/s 或 1000Mb/s。此外，级联还会增加延时，如图 9-1-2 所示级联中的 PC1 要访问 PC2，PC1 把数据帧发给交换机 S1，S1 查询本地的 MAC 地址表，把数据帧转发给交换机 S2，S2 再查询本地的 MAC 地址表，把数据帧转发给 PC2，级联的交换机越多，查询 MAC 地址表的次数越多，花费的时间越长。

堆叠是通过专门的堆叠模块和堆叠线缆，把多台交换机堆叠在一起，相当于仍是一台交换机，只不过端口的数量增加了。堆叠线缆的速度一般都在 1000Mb/s 以上。但堆叠线缆长度一般都不超过 1 米，堆叠限制了网络的范围。堆叠比级联的速度要快，只需要查找一次 MAC 地址表，也就是查询总的 MAC 地址表。

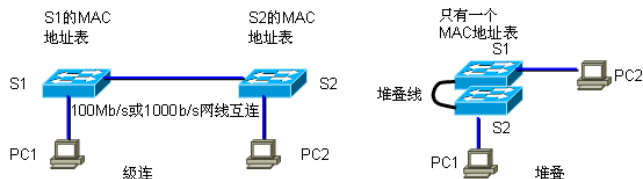


图 9-1-2 级联和堆叠

根据分级网络设计的要求，接入层交换机一般具备下面的特点：

- Port security（端口安全）。本章后面会介绍交换机的端口安全。
- VLAN（Virtual Local Area Network，虚拟局域网）。本书下一章介绍 VLAN 技术。
- 快速以太网或千兆位以太网。
- PoE（Power over Ethernet）。在以太网线上进行供电。
- Link aggregation（链路聚合）。属于 CCNP 的内容。
- QoS（Quality of Service，服务质量）。属于 CCNP 的内容。

典型的接入层交换机有 Catalyst 2950、Catalyst 2960 等二层交换机，当然也可以是三层或更高档的交换机。

汇聚层交换机一般具备下面的特点：

- 三层支持。三层交换机可以提供不同部门之间的互访。
- 高的转发速率。汇聚层连接着多个接入层交换机，要求比接入层有更高的速率，不然容易造成网络拥塞。
- 千兆位或万兆位链路。
- Redundant（冗余）功能。可以是链路冗余或设备冗余。
- Security Policies/Access Control Lists（安全策略和访问控制列表）。可以实现访问控制、策略路由等功能。
- Link aggregation（链路聚合）。
- QoS（服务质量）。

典型的汇聚层交换机有 Catalyst 3550-EMI、Catalyst 3560、Catalyst 3750 等三层交换机，当然也可以是档次更高的交换机。

核心层交换机一般具备下面的特点：

- 三层支持。
- 非常高的转发速率。
- 千兆位或万兆位链路。
- Redundant（冗余）功能。可以是链路冗余或设备冗余。
- Link aggregation（链路聚合）。
- QoS（服务质量）。

典型的核心层交换机有 Catalyst 4500、Catalyst 4900、Catalyst 6500 等三层交换机，当然也可以是档次更高的交换机。

至于选择什么型号的交换机，除了考虑到交换机的端口密度、转发速率、带宽聚合、功能（需要二层还是三层交换功能）、PoE 支持外，更主要的还要考虑到价格和企业的财力。



9.2 交换机分类*

交换机有多种分类方法。本节介绍交换机常见的几种分类方法。

9.2.1 根据转发方式分***

当交换机一个端口收到一个数据帧后，是等接收完整个数据帧后再转发，还是仅接收到部分数据帧后就开始转发。根据转发决定的早晚，交换分为 Store-and-Forward（存储转发）和 Cut-through。

（1）存储转发

在存储转发交换中，当交换机接收到数据后，交换机把数据存储在缓冲区中，直到接收了完整的帧。在存储转发过程中，交换机除了分析数据帧的目的地址外，还执行 CRC（Cyclic Redundancy Check，循环冗余检查）。CRC 检查失败的帧将被交换机丢弃。

（2）Cut-through

在 Cut-through 交换中，交换机接收到数据后即开始处理，并不需要等到完整地接收到

整个数据帧后再处理。交换机缓存数据帧的目的 MAC 地址，以便它能够确定从哪个或哪些端口转发数据。第 3 章介绍了以太网的帧格式，大家知道数据帧的前导位有 8 个字节，紧跟其后的就是 6 个字节的数据帧的目的 MAC 地址。交换机接收到数据帧的目的 MAC 地址后，就在 MAC 地址表中查找数据帧的目的 MAC 地址和对应的端口，然后把数据帧从对应的端口转发出去。在 Cut-through 交换中，交换机并不执行任何错误检查。因为交换机不必等待整个数据帧被完全缓存前就开始了转发，Cut-through 的交换速度比存储转发要快。但是，由于交换机不执行任何错误检查，一些错误的数据帧被在网络中传输，直至到达最终设备才会被丢弃。Cut-through 交换传输一些有错误的数据帧，浪费了网络的带宽。

Cut-through 交换有两种类型：

- **Fast-forward**（快速）转发：快速转发是收到一个数据帧的 14 个字节即开始转发。快速转发是典型的 Cut-through 交换方法。
- **Fragment-free**（无碎片式）转发：在无碎片式转发中，交换机接收到一个数据帧的 64 个字节时，开始转发数据帧。无碎片式转发，可以被看做是存储转发与 Cut-through 的折中。至于为何选择的是 64 个字节，这是因为大多数网络错误和碰撞过程都发生在前 64 个字节，也就是说，大多数的错误数据帧都小于 64 个字节。

! 注意：因为 Fast-forward 是典型的 Cut-through，所以很多文档中对交换机转发方式的分类是：Store-and-Forward、Cut-through、Fragment-free。

几种转发决定的位置如图 9-2-1 所示。

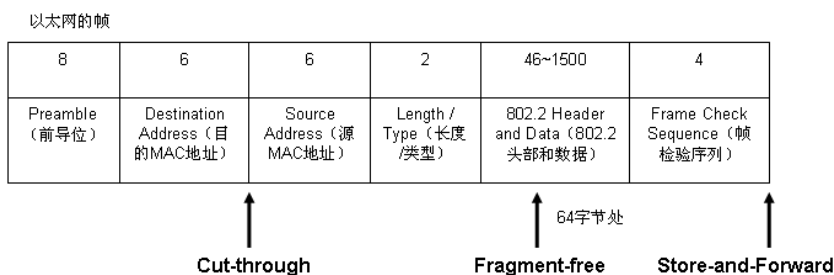


图 9-2-1 交换机转发决定的位置

表 9-2-1 对几种转发方式进行了对比。

表 9-2-1 转发方式对比表

	Cut-through	Fragment-free	Store-and-Forward
数据帧的转发延时	延时最小	延时居中	延时最大
错误检查能力	没有检查能力	检测能力居中	完整检查
收到多少字节开始转发	14	64	所有字节

9.2.2 根据对称性分*

根据交换机端口速度的不同，可以分为对称式（Symmetric）交换机和非对称式（Asymmetric）交换机。

（1）非对称式交换机

非对称式交换机的所有端口速率并不一样，比如多数都是 100Mb/s，少数几个端口是

1000Mb/s。快速的端口一般用来连接到主干或连接到服务器，用来克服链路的瓶颈。在非对称式交换机上要使用缓存空间，因为快速链路发往慢速链路的数据帧需要先被缓存下来，然后慢慢转发。这种交换机多用在 CS（Client/Server，客户/服务器）的网络中。

（2）对称式交换机

对称式交换机的所有端口速率都一样，这种交换机多用在 peer-to-peer（终端到终端）的网络中。为了解决上连链路的瓶颈问题，可以采用链路聚合技术，把多条慢速链路聚合成一条快速的链路。

为了提供更大的灵活性，当前多数交换机都被设计成非对称式交换机。

9.2.3 根据缓存方式分*

交换机根据转发方式分析部分或全部数据帧后，然后把数据帧发往目的地。在转发前，交换机需要存储数据帧；在目的端口拥塞时，交换机也需要存储数据帧。使用内存存储数据的方式叫做内存缓冲（memory buffering），根据缓存区划分的方式，有两种内存缓冲形式：基于端口和共享内存。

（1）基于端口内存缓冲

内存是基于每个端口分配的，每个端口都有固定的缓存空间，用来存储收到的数据包。

（2）共享内存缓冲

所有的端口共享一块内存，每个端口拥有的内存空间可以根据可用的共用内存空间来动态调整。

9.2.4 根据功能层分*

根据交换机所处的 OSI 功能层分，可以分为：二层交换机和三层交换机。

（1）二层交换机

根据 OSI 数据链路层（第二层）的 MAC 地址转发或过滤数据帧，处在 OSI 七层模型的第二层，所以也叫二层交换机。二层交换机对网络协议和用户应用程序是完全透明的。

（2）三层交换机

三层交换机不仅可以使第二层的 MAC 地址信息进行转发和过滤，还可以使用第三层的 IP 地址信息。三层交换机不仅学习 MAC 地址和对应的端口，还有能力执行第三层的路由功能。三层交换机处在 OSI 七层模型的第三层，所以叫三层交换机。

本书下一章，会介绍三层交换机和路由器的区别。



9.3 交换机基本配置**

本节介绍交换机的基本配置，交换机的很多配置与路由器的配置完全相同，对于相同的配置部分，本节不再重复，本节重点介绍交换机的 IP 地址和默认网关的配置。

9.3.1 与路由器的相似之处*

Cisco 支持两类主要的交换机操作系统：网络互联操作系统（IOS）和 Catalyst 操作系统（Cat OS）。目前，绝大多数 Cisco Catalyst 交换机系列都只运行 Cisco IOS，但是由于某些原因（思科公司最初是一个专业生产路由器的厂商，后来兼并了 Catalyst 交换机厂商，成

为全球最大的路由器和交换机生产厂商），一些高端 Cisco LAN 交换机既支持 Cisco IOS，又支持 Cat OS。对于 CCNA 考试，读者可以不管 Cat OS，而把注意力集中在 Cisco IOS 上。不过，需要记住的是，读者可能会看到像“基于 IOS 的交换机”这样的术语和用语，那指的是该交换机运行 Cisco IOS，而不是 Cat OS。

交换机与路由器的硬件组成相似，但交换机上没有 AUX（Auxiliary Port，辅助配置端口）。交换机的控制台连接与路由器的控制台连接一样，请参照本书的 4.3.1 节。

思科基于 IOS 的交换机的很多命令和操作与思科路由器完全一样。交换机也支持 Setup 模式，读者可以参照本书的 4.3.2 节。交换机的操作模式也分为用户模式、特权模式、全局配置模式、其他配置模式等，读者可以参照本书的 4.3.3 节。有关交换机中 CLI 在线帮助的使用、命令的简写、快捷键和高级编辑功能、历史命令缓存功能等的配置和使用与路由器相同，读者可以参照本书的 4.3.4 节。交换机的命名、旗帜的创建、时期和时间设置、密码配置、主机名列表配置、远程登录配置、DNS 配置等也与路由器的配置方法相同，读者可以参照本书的 4.3.5 节。

9.3.2 交换机的图形化管理工具

对思科交换机的配置除了使用 CLI 之外，还可以通过一些图形化的管理工具来实现。参加 CCNA 的考生只需了解有这么几款网管软件就可以了，作为网络工程师是需要会使用这几款软件的，毕竟多数的客户并不熟悉思科的 CLI。

（1）CNA（Cisco Network Assistant，思科网络助手）

CNA 软件可以免费从思科网站上下载，不过需要 CCO（Cisco Connection Online，思科在线连接系统）账号，思科合作伙伴和维护工程师才有 CCO 账号。CCNANEW.rar 的软件包中提供了 CNA 文件“cna-windows-k9-installer-5-3-en.exe”，CNA 是一款非常好用的思科交换机网管软件，但不属于 CCNA 考试的范畴，这里不再介绍。

（2）CiscoView

CiscoView 软件需要花钱购买，CiscoView 使用 SNMP（Simple Network Management Protocol，简单网络管理协议）可以设置交换机参数，并检查交换机的状态和性能信息。

（3）Cisco Device Manager

Cisco Device Manager 是一款基于 Web 的管理程序，该程序保存在交换机的内存中。可以使用 Cisco Device Manager 管理和配置交换机。

（4）SNMP Network Management

其他厂家开发的使用 SNMP 协议兼容的交换机管理软件，如 HP OpenView 等。

9.3.3 交换机的远程登录**

路由器任何一个接口均可以配置 IP 地址，交换机则不同，对于二层交换机来说，所有的端口都是二层端口，是不可以配置 IP 地址的；多数三层交换机，在默认情况下端口仍然是二层的，不可以配置 IP 地址，但可以通过命令，把二层的端口转变成三层的端口，就可以配置 IP 地址了。

所谓二层交换机，处在 OSI 七层模型的第二层，可以根据 MAC 地址进行过滤或转发，但不能根据 IP 地址实现路由转发。二层交换机虽然不能路由，但本身可以被配置一个 IP 地址，用来实现对交换机的远程管理。

读者打开 CCNA 模拟机架的拓扑图，在图中可以看到三台交换机，这三台交换机并不是真正的交换机，而是在思科 3640 路由器上添加了一块 16 口的交换模块，来完成 CCNA 考试中涉及的多数交换机实验。这里的模拟交换机与真实的交换机命令和功能有细微的差异，为了避免读者混淆，书中对有差别的地方均明确指出，以免影响读者在 CCNA 考试中的发挥。既然是在路由器上添加了交换模块，那么这里出现的交换机就是路由交换机了，有三层交换机的特性。对于一台三层交换机，如果没有配置它的三层特性，可以当成二层交换机来使用。

运行 CCNA 机架中的 R1 和 SW1，完成如图 9-3-1 所示的网络互连。

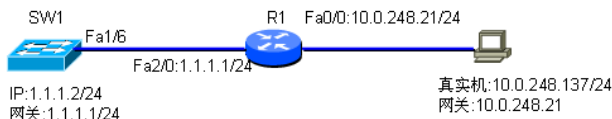


图 9-3-1 交换机的 IP 配置

R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#no cdp run
R1(config)#int fa 0/0
R1(config-if)#ip add 10.0.248.21 255.255.255.0
这里之所以使用 10.0.248.0/24 的 IP 地址，是因为笔者所在的局域网使用的就是这段 IP 地址。读者可以根据实际环境，改成任意网段的 IP 地址。
R1(config-if)#no shut
R1(config-if)#int fa 2/0
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config-if)#no shut
```

SW1 的配置和解释如下：

```
Router>
看到这个信息是不是吓了一跳，怀疑自己是不是开错了设备。从窗口最上面的“Connected to Dynamips VM "SW1" (ID 0, type c3600) - Console port”可以确认没有开错设备。可这里出现的为什么不是“Switch>”？前面已经解释过了，这里 SW1 并不是真正的交换机，而是在路由器上安装了交换模块，来实现交换机的部分功能，基本上可以完成 CCNA 考试涉及的所有实验配置。
Router#conf t
Router(config)#host SW1 既然看起来不像，那给它改成 SW1，至少看起来像了，人总是容易被外观假象迷惑。
SW1(config)#int fa 1/6 这里学一下路由器的配置，为交换机上连接路由器的 Fa1/6 接口配置 IP 地址。
SW1(config-if)#ip add 1.1.1.2 255.255.255.0 配置交换机 Fa1/6 接口的 IP 地址和子网掩码。

% IP addresses may not be configured on L2 links.
命令出错，提示 IP 地址不能被配置在一个二层的接口上。在默认情况下，即使是三层交换机上的端口也是二层端口，既然是二层端口，是不能配置 IP 地址的，而路由器路由模块上的端口默认都是三层端口，可以直接配置 IP 地址。
SW1(config-if)#int vlan 1
进入 VLAN1（虚拟局域网 1）。在默认情况下，交换机的所有端口都属于 VLAN1。VLAN 端口也称为虚拟路由端口，属于三层端口，可以配置 IP 地址。可以通过 VLAN 接口的 IP 地址对交换机进行远程管理。
SW1(config-if)#ip add 1.1.1.2 255.255.255.0 给 VLAN 接口配置 IP 地址。
SW1(config-if)#no shut
VLAN 接口属于三层端口。一个好习惯是对所有的三层端口，都使用“no shut”命令进行激活。而交换机上的二层端口在默认情况下都是激活的，不需要使用“no shut”命令进行激活，买来一台交换机，接上电脑就可以直接使用，因为交换机上所有的端口默认都是打开的。SW1 上的 Fa1/6 默认是一个二层接口，不需要使用“no shut”命令激活。
SW1(config-if)#exit
```

```
SW1(config)#no ip routing
```

二层交换机是不支持路由协议的，使用“no ip routing”命令关闭路由交换机的路由功能。

```
SW1(config)#ip default-gateway 1.1.1.1
```

对一台不支持路由协议的设备，配置默认路由的方法是配置一个网关。因为计算机默认不支持路由协议，配置的就是默认网关。对支持路由协议的设备，配置默认路由的方法是使用 ip route 0.0.0.0 0.0.0.0 的方法。

配置真实计算机的 IP 地址和默认网关，如图 9-3-1 所示。有的读者可能会觉得这样不方便，因为好多读者可能在看书做实验的同时，还开着 QQ、MSN 等程序，改变默认网关，意味着 QQ、MSN 都要断开。这里告诉读者一种两不误的方法，不要改变本来的默认网关，打开计算机的 DOS 窗口，如图 9-3-2 所示，在计算机上添加一条静态路由就可以了。



图 9-3-2 在计算机上添加静态路由

添加完静态路由后，计算机去往 1.1.1.2 的数据包是交给这里的虚拟路由器 R1 (10.0.248.21)，还是交给真实的网关设备 (10.0.248.1)？想一想，选路原则的第一条：最长匹配优先，静态路由的掩码长度是 24 位，默认路由的掩码长度是 0 位，所以去往 1.1.1.2 的数据包应该交给这里的虚拟路由器 R1 (10.0.248.21)。去往 QQ 或 MSN 服务器的数据包因为没有更明细的路由，就交给真实的网关设备 (10.0.248.1) 处理了。

在真实计算机上测试到 SW1 的连通性，测试如下：

```
C:\>ping 1.1.1.2
```

```
Pinging 1.1.1.2 with 32 bytes of data:
```

```
Reply from 1.1.1.2: bytes=32 time=12ms TTL=254
```

```
Reply from 1.1.1.2: bytes=32 time=11ms TTL=254
```

```
Reply from 1.1.1.2: bytes=32 time=16ms TTL=254
```

```
Reply from 1.1.1.2: bytes=32 time=11ms TTL=254
```

```
Ping statistics for 1.1.1.2:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 11ms, Maximum = 16ms, Average = 12ms
```

配置 SW1 支持远程登录，配置如下：

```
SW1(config)#enable password cisco
```

```
SW1(config)#line vty 0 4
```

```
SW1(config-line)#password cisco
```

```
SW1(config-line)#login
```

交换机远程登录的配置和路由器上的配置相同。在真实计算机上测试远程登录 SW1，显示如图 9-3-3 所示，可以成功进行远程登录。

因为 SW1 默认启用了 HTTP 服务，如果路由器或交换机没有启用 HTTP 服务，则可以使用下面的命令开启：

```
SW1(config)#ip http server
```

使用下面的命令关闭 HTTP 服务：

```
SW1(config)#no ip http server
```

开启 SW1 的 HTTP 服务后，在真实计算机的 IE 地址栏中输入 http://1.1.1.2，提示输入用户名和密码，保留用户名为空，在密码中输入使能密码，即可通过 Web 方式管理和查看交换机，如图 9-3-4 所示。

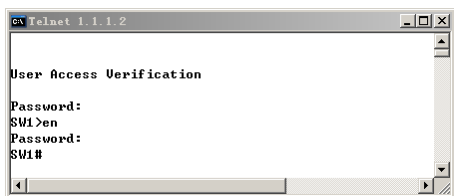


图 9-3-3 远程登录交换机成功

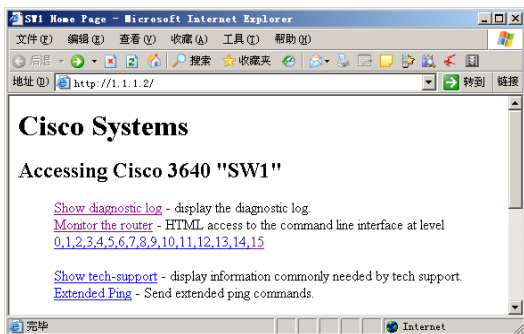


图 9-3-4 交换机的 Web 管理

9.3.4 交换机的维护和查看命令**

1. 配置文件的管理

(1) 保存配置文件

```
SW1#copy running-config startup-config
```

或

```
SW1#write
```

(2) 删除启动配置文件

```
SW1#erase startup-config
```

或

```
SW1#erase nvram:
```

(3) 备份文件到 TFTP 服务器

```
SW1#copy running-config tftp
```

或

```
SW1#copy startup-config tftp
```

(4) 从 TFTP 服务器恢复文件

```
SW1#copy tftp running-config
```

或

```
SW1#copy tftp startup-config
```

(5) 查看配置文件

```
SW1#show running-config
```

或

```
SW1#show startup-config
```

2. 查看路由表

查看 SW1 上的路由表，显示如下：

```
SW1#show ip route
```

```
Default gateway is 1.1.1.1
```

Host	Gateway	Last Use	Total Uses	Interface
ICMP redirect cache is empty				

因为 SW1 不再运行路由协议，所以这里显示的是默认网关。

3. 查看 MAC 地址表

查看交换机 SW1 的 MAC 地址表，显示如下：

```
SW1#show mac-address-table
Destination Address  Address Type  VLAN  Destination Port
-----
cc00.0464.0000      Self         1      Vlan1
ca07.0464.0038      Dynamic      1      FastEthernet1/6
```

从 MAC 地址表中，可以看出交换机从 Fa1/6 接口学到一个 MAC 地址，可以在路由器 R1 上执行 R1#show int fa 2/0 命令验证，该 MAC 地址就是路由器 R1 Fa2/0 接口的 MAC 地址。这里介绍一个小技巧，工作中路由器上的 MAC 地址可能有几百、几千条记录，想从中找出某一个 MAC 地址所在的端口，难度可想而知，通过使用过滤符的“show mac-address-table”命令，可以立即找出该 MAC 地址所对应的端口。下面的输出来自实际工作中的交换机。

```
Switch-4503#show mac-address-table | include 0030.18a6.bdf8
* 251 0030.18a6.bdf8 dynamic Yes 0 Gi1/21
```

显示只包含 MAC 地址“0030.18a6.bdf8”的行，立即找出该 MAC 地址所对应的端口了。

4. 查看 ARP 表

查看交换机 SW1 的 ARP 表，显示如下：

```
SW1#show arp
Protocol Address      Age (min)  Hardware Addr  Type  Interface
Internet 1.1.1.1        38        ca07.0464.0038 ARPA  Vlan1
Internet 1.1.1.2        -         cc00.0464.0000 ARPA  Vlan1
```

从这里可以看出 1.1.1.1 对应的 MAC 地址是 ca07.0464.0038。读者思考一个问题，如何从工作交换机的成百上千条记录中，找出某一个 IP 地址所对应的交换机端口。方法如下：

```
SW1#show arp | include 1.1.1.1
Internet 1.1.1.1        41        ca07.0464.0038 ARPA  Vlan1
SW1#show mac-address-table | include ca07.0464.0038
ca07.0464.0038      Dynamic      1      FastEthernet1/6
```

上述的解决办法是先找到该 IP 地址所对应的 MAC 地址，再找到该 MAC 地址所对应的端口。如果交换机的 ARP 表中没有出现相应的条目，可以先在交换机上 ping 一下对应的 IP 地址。



9.4 交换机的安全配置**

本节介绍交换机的密码安全和易受到的安全威胁，以及对应的保护措施。

9.4.1 交换机密码安全*

为了加强交换机自身的安全，需要配置交换机 Console 端口登录密码、VTY 登录密码和 Enable 密码，加密所有的密码和取消密码加密，交换机的配置与路由器的配置完全相同，这里就不多叙述了。交换机的密码恢复请参阅本书 18.5.2 节。

9.4.2 交换机易受到的安全威胁*

交换机比集线器的安全性虽有所提高，但仍然无法阻止一些恶意攻击。

1. MAC 地址泛洪（Flooding）

在前面的学习中，读者已经了解到交换机的工作原理，即根据数据帧中的源 MAC 地址进行学习，根据数据帧中的目的 MAC 地址进行转发。由于交换机的型号不同，MAC 地址表中可容纳的 MAC 地址数量也不同，在正常情况下，MAC 地址表的容量是足够使用的。

如果有一台攻击主机，通过程序伪造大量包含随机源 MAC 地址的数据帧发往交换机，有些攻击程序一分钟内可以发出十几万个伪造的 MAC 地址，交换机根据数据帧中的源 MAC 地址进行学习，一般交换机的 MAC 地址表容量也就几千条，交换机的 MAC 地址表瞬间被伪造的 MAC 地址爆满。交换机的 MAC 地址表容量已满，交换机再收到数据帧，不管是单播、组播还是广播，交换机都不再学习 MAC 地址。如果交换机在 MAC 地址表中找不到目的 MAC 地址对应的端口，交换机将会和集线器一样，向所有端口广播数据帧，而不管是单播、组播还是广播数据帧，只要在攻击主机上安装网络捕获软件，如 Sniffer 之类，就可以捕获网络流量，加以分析，从而达到窃听的目的。

MAC 地址表有一个老化时间，默认是 5 分钟，如果交换机在 5 分钟之内没有再收到一个 MAC 地址表条目的数据帧，交换机将从 MAC 地址表中清除这个 MAC 地址条目；如果收到，则刷新 MAC 地址表老化时间。为了保证这种攻击总是有效，攻击主机必须持续不断地发动 MAC 地址攻击。

2. DHCP 欺骗（Snooping）

如图 9-4-1 所示，在没有 DHCP 欺骗的情况下，DHCP 客户机可以从合法 DHCP 服务器获取到正确的 IP 地址、子网掩码、网关和 DNS。如果网络中被安插了一台非法的 DHCP 服务器，该服务器可以任意向外分配地址，在图 9-4-1 中，非法的 DHCP 服务器离 DHCP 客户端更近，DHCP 客户端更容易获取到非法 DHCP 服务器分配的假 IP 地址。

如果非法 DHCP 服务器仅是随便分配 IP 地址，影响用户的正常上网，并没有攻击意图，危害还不算大。如果攻击者分配假的网关，比如把网关指向一台攻击主机，客户机

首先把网络流量发往攻击主机，攻击主机再把网络流量转发给真正的网关，这样虽然不影响客户机的上网，但客户机的所有网络流量都流经攻击主机，很容易泄露一些机密信息，这种攻击也叫中间人攻击。

如果非法 DHCP 服务器分配一个恶意的 DNS 服务器，在 DNS 服务器上再配置一个错误的域名，比如把中国人民银行的网址映射成一个攻击主机的 IP 地址，在攻击主机上再做一个假的中国人民银行 Web 页面，很容易就可以捕获到用户的账号和密码信息。读者千万不要尝试这种攻击，否则下半辈子可能就要在监狱中度过了。



图 9-4-1 DHCP 欺骗

3. CDP 攻击

CDP 是思科的设备发现协议，在默认情况下，所有的思科路由器和交换机都运行 CDP 协议。CDP 是一个二层协议，被广播发送，不使用验证和加密，攻击者可以从 CDP 消息中，查看到思科设备的 IP 地址和 IOS 版本等信息。有些 IOS 中可能会存在一些 Bug，攻击者可以利用 Bug 对思科设备发动攻击。建议禁用 CDP 协议。

4. 密码暴力破解

针对密码暴力破解的方法，可以设置一个复杂的密码，并经常更换密码。

5. 远程登录攻击

使用 Telnet 可以对交换机进行远程管理，但 Telnet 使用的是明文传输，也就是密码也会被明文传输，攻击者捕获这样的报文后，可以获知交换机的管理密码。建议使用更安全的协议对交换机进行远程管理，比如 SSH，本书第 18 章介绍了禁用 Telnet，使用 SSH 的配置。

6. DoS 攻击

攻击者可以进行 DoS（Deny of Service，拒绝服务）攻击，发动对交换机上 Telnet 服务的攻击，造成交换机不能对管理员的 Telnet 操作进行响应。解决的办法就是升级交换机的 IOS 软件，在新版的 IOS 软件中，包含有针对 DoS 攻击的补丁。

7. ARP 攻击

ARP（Address Resolution Protocol，地址解析协议）攻击是目前局域网中危害最大、影响最深的网络攻击手段，并在网上有很多 ARP 攻击软件可供下载，有了这些攻击软件，一个菜鸟也可发动对网络的攻击。思科考试中虽不涉及 ARP 欺骗及解决办法，可是作为一名 CCNA，如果连 ARP 攻击都不明白，也解决不了，那就不是一名合格的 CCNA，甚至称不上是合格的网管。下面看一下 ARP 攻击的原理。

（1）以太网的工作原理

在以太网中，数据包被发送出去之前，首先要进行拆分（把大的包进行分组）、封装（在网络层添加源 IP 地址和目标 IP 地址，在数据链路层添加源 MAC 地址和下一跳的 MAC 地址），变成二进制的比特流。以太网中数据的传输仅知道目标的 IP 地址是不够的，还需要知道下一跳的 MAC 地址，这需要借助于另外一个协议——ARP（地址解析协议）。

（2）ARP 的工作原理

在 ARP 查询包中：“以太网目的地址”为 0xffffffff 广播地址；“以太网源地址”为本机网卡的 MAC 地址；“帧类型”为 0x0806，表示 ARP 应答或请求；“硬件类型”为 0x0001，表示以太网地址；“协议类型”为 0x0800，表示 IP 地址；“OP”为 ARP 的请求或应答，ARP 请求包的 OP 值为 1，ARP 应答包的 OP 值为 2；“发送端以太网地址”为发送者的 MAC 地址；“发送端 IP”为发送者的 IP 地址；这里“目的以太网地址”为 0x000000000000；“目的 IP”为查询 MAC 地址的 IP 地址。此包以广播形式发送到网络上，局域网中所有的计算机均收到此包，只有本机 IP 地址为“目的 IP”的计算机对此包进行响应，并回复此包。当“发送端”收到此 ARP 应答包后，即获取到目标 IP 地址对应的 MAC 地址，然后就可进行数据包的封装了。

（3）ARP 攻击类型

了解 ARP 的工作原理后，只要有意图地填充某些字段，即可达到 ARP 攻击的效果。如 IP 地址冲突、ARP 欺骗、ARP 攻击等。

- **IP 地址冲突：**ARP 攻击者利用这一原理，用任意的 MAC 地址（非被攻击者真实的 MAC 地址）填充“发送端以太网地址”字段，用被攻击者的 IP 地址填充“发送端 IP”字段，用被攻击者的真实 MAC 地址填充“目的以太网地址”字段，用被攻击者的 IP 地址填充“目的 IP”字段，OP 的值为“2”。当被攻击者收到这样的 ARP 应答后，就认为本机的 IP 地址在网络上已经被使用，弹出 IP 地址冲突对话框。

- **ARP 欺骗**: 用错误的 MAC 地址和 IP 地址对应起来欺骗其他主机, 使其他主机网络访问失败。目前网络上常见的就是这样一种攻击, 用网关 IP 地址和错误的 MAC 地址向外宣告, 使被欺骗主机网络访问失败。目前网络上流行的“网络执行官”等软件就可发动 ARP 欺骗, 断开目标主机的网络访问。
- **ARP 攻击**: 用本机的 MAC 地址和被欺骗的 IP 地址向外宣告, 从而达到欺骗目标主机的目的, 起到中间人攻击的效果。目前网络上流行的“Cain”等软件就可发动 ARP 攻击, 从而进一步捕获目标主机的敏感信息。

9.4.3 交换机的安全防护*

针对交换机易受到的安全威胁, 这里给出一些解决办法。

1. MAC 地址泛洪的解决办法

针对 MAC 地址泛洪, 可以配置交换机的端口安全。限制交换机每个端口可以学习的 MAC 地址数量, 这样攻击主机即使伪造很多的源 MAC 地址, 交换机也只学习有限的 MAC 地址。Dynamips 模拟机架不支持交换机端口安全的配置, 下面的配置是 Packet Tracer 模拟器的思科 2960 交换机上完成的。

```
Cisco2960(config)#int fa 0/6          进入需配置端口安全的端口。
Cisco2960(config-if)#switchport mode access
把交换机端口配置成接入端口。端口安全只能配置在二层的接入端口上, 也就是说, 三层的交换机端口或二层
的主干端口都是不支持交换机端口安全的。本书下一章会介绍到主干端口。
Cisco2960(config-if)#switchport port-security
启用交换机端口的端口安全, 启用交换机端口安全后, 该接口默认只学习一个 MAC 地址。
```

配置交换机的端口安全后, 可以有效地防止 MAC 地址泛洪攻击。配置了端口安全的交换机端口, 如果从端口收到了第二个源 MAC 地址的数据帧, 交换机将关闭该端口。这感觉有点像古代的“连坐”, 一个人犯罪, 亲人都要跟着遭殃。每个端口只允许学习一个 MAC 地址, 用户想级联交换机或集线器都不可以, 有点太不近人情了, 通过下面的命令, 来更改端口可以学习的 MAC 地址数量。

```
Cisco2960(config-if)#switchport port-security maximum ?
<1-132> Maximum addresses
可以看到该端口最大可以支持 132 个 MAC 地址, 不同型号的交换机该数值是不同的。不管配置交换机端口的
什么安全特性, “switchport port-security”命令都是要配置的, 这相当于端口安全的配置开关。
Cisco2960(config-if)#switchport port-security maximum 100    配置该端口可以学习 100
                                                                个 MAC 地址。
```

古代的“连坐”尽管可以有效地降低犯罪, 但一直没有被现在的法律所采用。因为一个非法用户的接入, 而让所有的合法用户上不了网, 这样的处罚似乎有点儿重了。在交换机上也取消“连坐”, 改成其他处理方式吧:

```
Cisco2960(config-if)#switchport port-security violation ?
protect    Security violation protect mode
restrict   Security violation restrict mode
shutdown   Security violation shutdown mode
违反安全规定将采取的动作。违反安全规定的行为包括: 当交换机端口最大的 MAC 地址数已经达到, 又有新的
MAC 地址被学到时; 当一个地址被配置在一个安全端口上, 结果从另一个安全端口也学到同样的 MAC 地址时。
采用的动作可以有三种, 默认是 shutdown, 关闭端口的同时, 还发送日志消息, 违反计数器值增加。如果选
择 protect (保护), 交换机将对违反的行为不支持, 比如不学习新的 MAC 地址, 但也不会关闭端口。如果选
择 restrict (约束), 动作与 shutdown 差不多, 会发送日志消息, 违反计数器值也增加, 但不关闭端口。
Cisco2960(config-if)#switchport port-security violation restrict
这里选择有违反行为发生时, 动作是约束。
```

交换机上支持一次配置多个端口。比如配置交换机的 fa 0/1、fa 0/2、fa 0/3、fa 0/4、fa 0/5、fa 0/7、fa 0/9、fa 0/10、fa 0/11、fa 0/12、fa 0/13、fa 0/14、fa 0/15 端口启用端口安全，每个端口最大允许的 MAC 地址数目是 10，违反规定的动作是约束。配置如下：

```
Cisco2960(config)#int range fa 0/1 - 5,fa 0/7,fa 0/9 - 15
连续的1到5号端口可以写成 fa 0/1 - 5，比如配置交换机的前20个端口，则可以写成 fa 0/1 - 20。
如果是不连续的端口，需要加逗号分开，用逗号分开后，端口的类型要写明，比如这里的 fa 0/7，fa 不可以省略。
Cisco2960(config-if)#switchport mode access
Cisco2960(config-if-range)#switchport port-security          打开端口安全开关。
Cisco2960(config-if-range)#switchport port-security maximum 10
                                                                最大允许10个MAC地址。
Cisco2960(config-if-range)#switchport port-security violation restrict
                                                                违反的动作是约束。
```

交换机端口安全中还包括 MAC 地址绑定，比如下面的配置把 MAC 地址“0019.566e.153f”绑定在交换机的 fa 0/1 端口，不允许从其他安全端口学习到这个 MAC 地址。

```
Cisco2960(config)#int range fastEthernet 0/1-23
Cisco2960(config-if)#switchport mode access
Cisco2960(config-if-range)#switchport port-security
Cisco2960(config-if-range)#switchport port-security maximum 10
Cisco2960(config-if-range)#exit
Cisco2960(config)#int fa 0/1
Cisco2960(config-if)#switchport port-security mac-address 0019.566e.153f
```

有时手工绑定交换机端口上的 MAC 地址，工作量比较大，可以使用下面的命令让交换机端口自动绑定学到的 MAC 地址。

```
Cisco2960(config)#int fa 0/1
Cisco2960(config-if)#switchport port-security
Cisco2960(config-if)#switchport port-security mac-address sticky
让交换机端口自动学习端口的MAC地址，粘贴的MAC地址将出现在运行的配置文件中，如果以后都需要这样的值，可以把运行配置文件保存起来。
```

可以使用“show port-security interface”命令查看交换机端口安全的设置和违反规定计数器值。显示如下：

```
Cisco2960#show port-security int fa 0/1
Port Security          : Enabled
Port Status            : Secure-down
Violation Mode         : Restrict
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 10
Total MAC Addresses    : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

可以使用“show port-security”命令查看所有配置了端口安全的交换机端口的最大允许 MAC 地址数、当前学到的 MAC 地址数、违反了安全规则多少次、违反规定的动作等。部分显示如下：

```
Cisco2960#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)        (Count)        (Count)
-----
Fa0/1        1          0             0             Shutdown
Fa0/2        1          0             0             Shutdown
Fa0/3        1          0             0             Shutdown
-----
```

光盘中的“补充资料\实验 2.pdf”文件介绍了通过修改 MAC 地址来实现 IP 地址盗用,利用本节介绍的配置交换机的端口安全可以杜绝这类违规行为。

2. DHCP 欺骗的解决办法

可以配置交换机来防止 DHCP 欺骗, Dynamips 和 Packet Tracer 模拟器都不支持 DHCP 防欺骗功能。真实思科 2960 交换机的配置如下:

```
Cisco2960(config)#ip dhcp snooping
启用交换机的 DHCP 欺骗功能。启用该功能后, 交换机会构造一个 DHCP 的绑定表, 表中会记录一个客户端的
MAC 地址和对应的 IP 地址、VLAN 号和端口号。
Cisco2960(config)#ip dhcp snooping vlan 1    在 VLAN1 上启用 DHCP 欺骗功能。
Cisco2960(config)#int fa 0/24
启用 DHCP 欺骗功能后, 在默认情况下交换机上的所有端口都是不信任端口, 不信任端口不接收 DHCP 的应答消息。需要把交换机之间的互连端口和连接合法 DHCP 服务器的端口配置成信任端口。图 9-4-2 中画圈的交换机
端口需要被配置成信任端口。
Cisco2960(config-if)#ip dhcp snooping trust 信任端口可以接收 DHCP 的应答消息。
Cisco2960(config-if)#int range fa 0/1 - 23
Cisco2960(config-if-range)#ip dhcp snooping limit rate 2
这是一个可选配置。限制非信任端口发送 DHCP 请求包的速率, 避免非法用户大量发送 DHCP 请求包, 耗尽 DHCP
服务器地址池中的可用 IP 地址。
```

经过上述配置后, 非法 DHCP 服务器的 DHCP 响应报文被交换机阻止, 不会影响整个网络的 IP 地址分配。此外, 在 CCNP 中会介绍 DAI (Dynamic ARP Inspection, 动态 ARP 检查), 在 DAI 中需要使用 DHCP 欺骗技术构建的 DHCP 绑定表, 来有效地阻止 ARP 欺骗。

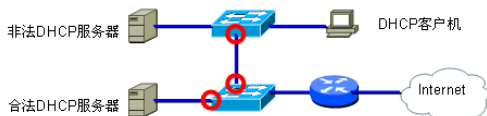


图 9-4-2 配置 DHCP 欺骗的信任端口

3. ARP 攻击的解决办法

ARP 攻击的解决办法是选读部分, 不属于 CCNA 考试的范畴, 但在实际工作中却相当实用。

(1) 如何判断正在遭受 ARP 攻击

有用户反映, 昨天还能上网的, 今天却不能上网了; 刚刚还能上网的, 现在却不能上网了; 有的人不能上网, 但接在同一台交换机上的其他人却可以上网; 一会儿能上网, 一会儿不能上网等诸如此类的问题。

判断是否存在 ARP 攻击的方法比较简单:

① 在出现问题的计算机的运行框中输入“ping 192.168.1.1 -t”, ping 是一个 DOS 命令, 用来测试网络的连通性; 192.168.1.1 指网关, 实际生活中换成用户的网关或者不能访问的同一网段的目标计算机的 IP 地址; 在正常情况下, ping 命令只测试 4 个包就结束, -t 的意思就是一直测试, 直到人为干预才停止。如果正在遭受 ARP 攻击, 屏幕将会提示“Request time out”。但反之却不一定, 比如目标计算机启用防火墙软件或网关设备拒绝 ping 等也会出现“Request time out”提示。

② 在受害计算机上开启另外一个 DOS 窗口, 输入“arp -d”, arp 是一个 DOS 命令, 能解析出 IP 地址对应的网卡 MAC 地址, -d 用来清除本机缓存的所有 IP 地址和 MAC 地址的对应。如果发现①中的窗口内容变成持续的“Reply from.....”, 则表示曾遭受过 ARP 攻击, 现在已经正常了; 如果仅出现了一个“Reply from.....”包, 后面又变成了“Request time out”包, 则表明该计算机正在遭受持续不断的 ARP 攻击。当前网上有很多 ARP 攻击软件可以下载, “网络执法官”就是其中的一种。

(2) ARP 攻击的解决办法

ARP 攻击的解决办法可谓五花八门，但却因为很多的限制，最终可以实施的却凤毛麟角，甚至连一种可以实施的都找不到。下面的解决办法虽然谈不上包罗万象，但不管用户的网络硬件配备如何，一定可以从中找到一种最适合的解决办法。

① 在上面的判断过程中已经发现存在 ARP 攻击，如果攻击持续存在，在受害的计算机上执行“arp -d”后，再执行“arp -a”，-a 的作用是显示该计算机上的所有 ARP 缓存。从中我们可能会发现有几条记录，其中一个记录是网关或要访问的目标主机，还有一条其他的记录，也可能有几条。多执行几次“arp -d”、“arp -a”，总结一下，出现最多的那条记录基本上就是 ARP 攻击者的真实 IP 地址。

该方法的优点：方法比较简单，几乎适合所有的网络环境，不需要任何辅助软件，也不需要网管有非常专业的知识，即可找出攻击者，然后对攻击者进行网络隔离。缺点：如果攻击者仅仅是破坏，而不是出于控制的目的，“arp -a”看到的记录就不可靠了。

② 在目标设备和受害计算机上分别进行 IP 地址和 MAC 地址的静态绑定。比如，在计算机上执行“arp -s 192.168.1.1 00-aa-00-62-c6-09”；在路由或交换设备上执行“Cisco-6509(config)# arp 192.168.1.2 0009.6be2.3ca3 ARPA”，这里仅以思科的设备为例。把要保护的目标设备的 IP 地址和 MAC 地址进行绑定，使非法的 ARP 攻击无孔可入。

该方法的优点：这是目前介绍最多的方法，对小规模网络比较适用。缺点：具体实施的难度比较大，如果上网主机比较多，并且主机经常变化，比如高校这一群体，静态绑定工作量巨大，难以实施；太多的绑定条目会影响设备的执行速度，降低效率；即使 ARP 攻击不会影响上网，但大量的 ARP 包仍被发送，还是要占用大量的有用带宽；要求设备支持静态绑定功能。

③ 采用动态的 ARP 检查技术，结合 DHCP 的功能，实现 IP 地址和 MAC 地址的自动绑定。该方法和②类似，但绑定是自动完成的，可以在接入层交换机上部署，非法的 ARP 包将被交换机丢弃，CCNP 中会介绍这种技术。感兴趣的读者，请查找对应设备的技术文档。

该方法的优点：这是解决 ARP 攻击最好的方法，不需要管理人员的协助，非法的 ARP 包也无法进入网络，既不会存在危害，也不会影响网络性能。缺点：要求管理员有较好的技术；要求网络设备的支持，思科公司支持这种功能的设备至少要三层以上（国内很少有企业在接入层使用三层设备），很多厂家的设备目前尚未支持。

④ 在网管型交换机上，用一分钟的时间即可找出攻击者。在前面的解决方法①中，可以发现目标 IP 地址的 MAC 地址并不是真实的 MAC 地址，记下这个 MAC 地址，假使这个 MAC 地址是“0050.bae3.2305”，在网管型交换机上执行：

```
Cisco-2950#show arp | include 0050.bae3.2305
Internet 10.168.168.9          239 0050.bae3.2305 ARPA FastEthernet1/17"
```

第一行是执行的命令，单纯的“show arp”会显示出交换机学习到的所有 MAC 地址，从中找到攻击 MAC 地址非常困难；“| include 0050.bae3.2305”起到过滤功能，仅显示对应的行。第二行是执行结果，我们发现这个 MAC 地址来自 1/17 端口，找到该端口对应的主机即找到了攻击源。如果该端口连接的不是一台计算机，而是另一台交换机，重复刚才的方法，直到找出最终的计算机。

该方法的优点：该方法最具有可操作性，执行比较快捷，所有的网管型交换机均支持该功能，强烈推荐使用。缺点：毕竟很多单位还使用着非网管型交换机或集线器。

⑤ 在非网管型交换机或集线器的情况下，用 10 分钟的时间即可找出攻击者。在被攻击者的计算机上打开两个 DOS 窗口，一个窗口执行“ping 192.168.1.1 -t”，另一个 DOS 窗口中间隔性执行“arp -d”，如果有多台非网管型交换机或集线器，依次切断它们的电源，何时发现第二个 DOS 窗口中出现持续的“Reply from.....”，则可以断定 ARP 攻击源来自这台网络设备。接下来恢复该设备的电源，把网线一根根地拔下来，何时发现第二个 DOS 窗口中出现持续的“Reply from.....”，则可以断定该网线所接的设备就是 ARP 攻击源。如果嫌这种查找方法慢，可以使用二分查找法，即一次拔下一半的线，测一下，一般不超过 10 分钟即可找出攻击源。

该方法的优点：几乎适合任何网络环境。缺点：执行起来有点困难。

⑥ 作为网络中心的一名网管解决的办法有很多种，可作为一名普通的网络用户除了抱怨之外，有什么切实可行的办法呢？编写下面的批处理文件，在用户的计算机上执行，即可解决 ARP 的攻击问题。批处理文件的内容如下：

```
: a
Arp -d
Ping 1.1.1.1 -n 1 -w 100
Goto a
```

把该文本文件保存为 a.bat，然后在用户的计算机上双击执行，会打开一个 DOS 窗口，程序会循环执行，不要关闭该窗口即可解决 ARP 攻击问题。如果嫌 ARP 清除的速度太慢，可以改变上面的 100（表示 0.1 秒）为想要的时间。

该方法的优点：非网管人员的自救办法。缺点：频繁地清除 ARP 缓存，广播 ARP 查询包，不仅会影响计算机的性能，也会加重网络的负担。

⑦ 安装 ARP 防火墙。下载第三方的 ARP 防火墙软件，目前使用比较多的是免费版的 360 防火墙。这种软件的原理类似方法⑥。



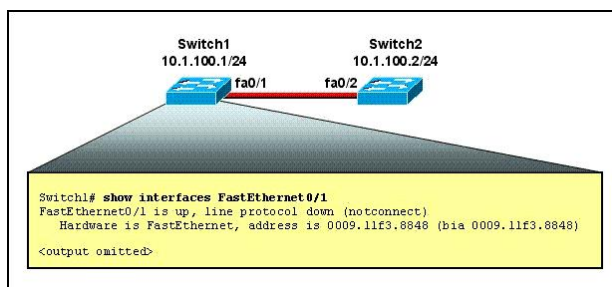
9.5 真题精选***

1. While troubleshooting a connectivity problem, a network administrator notices that a port status LED on a Cisco Catalyst series switch is alternating green and amber. Which condition could this indicate?

- A. The port is experiencing errors.
- B. The port is administratively disabled.
- C. The port is blocked by spanning tree.
- D. The port has an active link with normal traffic activity.

2. Refer to the exhibit. The network administrator has verified that a functioning cable connects Switch1 and Switch2. From the output that is shown, what two pieces of information can the administrator validly conclude? (Choose two.)

- A. Using a source MAC address of 0009.11f3.8848, Switch2 is sending frames to Switch1.
- B. Interface fa0/1 on Switch1 is in a shutdown state.
- C. The status of fa0/2 should be checked on Switch2.
- D. There is likely to be an IP address issue on Switch1 fa0/1.
- E. The interface is functional at OSI Layer 1.



3. In order to complete a basic switch configuration, drag each switch IOS command on the left to its purpose on the right.

ip default-gateway	allows access to high-level testing commands, such as debug
interface vlan 1	allows access to configuration commands that affect the system as a whole
hostname	sets the system name
ip address	activates the interface configuration mode for VLAN 1
enable	enables the switch management interface
no shutdown	sets the switch management IP address
configure terminal	allows the switch to be managed from remote networks

Drag and drop question. Drag the items to the proper locations.

4. Why would a network administrator configure port security on a switch?

- A. to prevent unauthorized Telnet access to a switch port
- B. to limit the number of Layer 2 broadcasts on a particular switch port
- C. to prevent unauthorized hosts from accessing the LAN
- D. to protect the IP and MAC address of the switch and associated ports
- E. to block unauthorized access to the switch management interfaces over common TCP ports

5. A network administrator wants to ensure that only the server can connect to port Fa0/1 on a Catalyst switch. The server is plugged into the switch Fa0/1 port and the network administrator is about to bring the server online. What can the administrator do to ensure that only the MAC address of the server is allowed by switch port Fa0/1?

- A. Configure port Fa0/1 to accept connections only from the static IP address of the server.
- B. Employ a proprietary connector type on Fa0/1 that is incompatible with other host connectors.
- C. Configure the MAC address of the server as a static entry associated with port Fa0/1.
- D. Bind the IP address of the server to its MAC address on the switch to prevent other hosts from spoofing the server IP address.
- E. Configure port security on Fa0/1 to reject traffic with a source MAC address other than that of the server.

- F. Configure an access list on the switch to deny server traffic from entering any port other than Fa0/1.
6. The network security policy requires that only one host be permitted to attach dynamically to each switch interface. If that policy is violated, the interface should shut down. Which two commands must the network administrator configure on the 2950 Catalyst switch to meet this policy? (Choose two.)
- A. Switch1(config-if)# switchport port-security maximum 1
 - B. Switch1(config)# mac-address-table secure
 - C. Switch1(config)# access-list 10 permit ip host
 - D. Switch1(config-if)# switchport port-security violation shutdown
 - E. Switch1(config-if)# ip access-group 10
7. Which two passwords must be supplied in order to connect by Telnet to a properly secured Cisco switch and make changes to the device configuration? (Choose two.)
- A. console password
 - B. vty password
 - C. aux password
 - D. tty password
 - E. enable secret password
 - F. username password



9.6 真题解答***

1. 解：A

题目问：当排除连接问题时，网络管理员注意到思科 Catalyst 系列交换机有一个端口交替显示绿色和琥珀色（黄色），指示了什么情形？Cisco 交换机的端口状态指示灯在绿色和琥珀色（黄色）间交替，表示端口有操作的问题——也许是过量的错误或连接的问题。B 选项说交换机的端口被关闭，如果被关闭，该端口的指示灯是熄灭的；C 选项说该端口被生成树协议（生成树协议本书稍后会介绍到）阻塞，被生成树协议阻塞的端口显示持续的琥珀色；D 选项说端口在活路的链路上，有正常的流量经过，端口正常时的颜色是绿色，如果有流量经过，将是闪烁的绿色。

2. 解：CE

题目问：参照图，网络管理员已经检查到 Switch1 和 Switch2 之间的连接线缆，从图中的输出，管理员可以得出哪两个合法的结论？端口显示为 notconnect，当然需要检查对端的端口状态了。一般来说，交换机的端口显示为前面的 up，后面的 down，是数据链路层的问题。因为物理层是 OSI 的第一层，所以说它工作在 OSI 的第一层。A 选项中，0009.11f3.8848 是 Switch1 上的 MAC 地址，Switch2 不可能用这个地址作为源地址；B 选项说 Switch1 的 Fa0/1 端口被关闭，被关闭的端口显示的是“administratively down”；D 选项说可能是 Switch1 的 Fa0/1 端口的 IP 地址问题，二层交换机端口不能配置 IP 地址，三层交换机端口可以配置 IP 地址，但交换机端口显示“notconnect”与端口的 IP 地址无关。

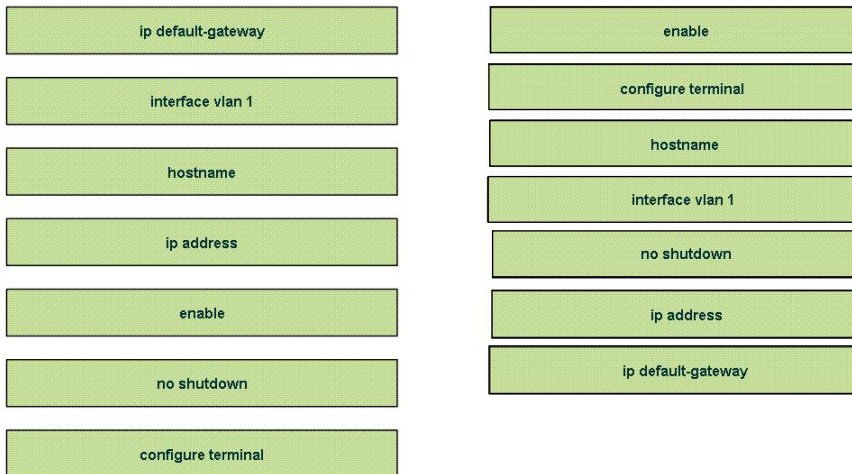
3. 解：

正确结果如下图所示：

题目要求：为了完成交换机的基本配置，把左边的每一个交换机 IOS 命令拖到右边合

适的位置。根据右边图中的要求，交换机的配置命令如下：

Switch>enable	进入特权模式，特权模式可以访问更高级别的命令，比如 debug。
Switch#configure terminal	进入全局配置模式，配置命令影响整个系统。
Switch(config)#hostname ccna	配置交换机的名字。
ccna(config)#interface vlan 1	激活 VLAN 1 的接口配置模式。
ccna(config-if)#no shutdown	启用交换机的管理端口。
ccna(config-if)#ip add 1.1.1.1 255.255.255.0	配置交换机的管理 IP 地址。
ccna(config)#ip default-gateway 1.1.1.254	给交换机配置网关后，允许从远程网络管理交换机。



4. 解：C

题目问：网络管理员为什么愿意配置交换机的端口安全？配置端口安全可以限制交换机端口接受的 MAC 地址数，限制交换机端口可以接受特定的 MAC 地址等保护网络，限制未授权的用户访问网络。此题用排除法较好，A 选项说阻止没有授权的 Telnet 访问端口，交换机的端口安全是没有办法阻止 Telnet 访问的。本书的访问控制列表一章，会介绍到，可以在 VTY 端口挂接访问控制列表，来阻止未授权的 Telnet 访问；B 选项说在特定的交换机端口上限制第二层的广播，不管是否配置端口安全，二层交换机端口都转发广播，端口安全对广播没有影响；C 选项说阻止没有授权的主机访问网络是正确的；D 选项说保护交换机相关端口的 IP 地址和 MAC 地址，安全端口只能保护 MAC 地址，不能保护 IP 地址；E 选项说阻止没有授权的访问交换机管理端口的 TCP 端口，端口安全是第二层接入端口的功能，不涉及第四层的 TCP 端口。

5. 解：CE

网络管理员想确保只有服务器能连接到交换机的 Fa0/1 端口，管理员做什么可以确保交换机的 Fa0/1 端口只允许服务器的 MAC 地址？要实现交换机的 Fa0/1 端口上仅仅允许转发服务器 MAC 地址的流量，可以配置将服务器的 MAC 地址和交换机的端口进行绑定，并拒绝其他 MAC 地址的流量。交换机的配置步骤如下：

Switch(config)#int fa 0/1	进入服务器的交换机端口。
Switch(config-if)#switchport mode access	只有接入端口才可以配置端口安全。
Switch(config-if)#switchport port-security	启用端口安全。
Switch(config-if)#switchport port-security violation restrict	
有违例操作时，限制操作，默认的是 shutdown，这里一定要改，不然有一个非法的 MAC 地址进入，将会导致交换机端口关闭，此时合法的服务器 MAC 地址也无法使用网络了。	

```
Switch(config-if)#switchport port-security mac-address 0002.e332.7e4f
```

在这个端口上静态绑定服务器的 MAC 地址。

```
Switch(config-if)#switchport port-security maximum 1
```

限制该交换机端口只允许一个 MAC 地址，这是启用交换机端口安全的默认配置，可以省略该配置，如果该端口要绑定多个 MAC 地址，则需更改允许的 MAC 地址数。

A 选项说在交换机端口上配置静态的 IP 地址绑定，二层交换机无法绑定三层的 IP 地址。B 选项说使用一个私有的与其他主机不兼容的连接类型，这未免花费也太高了。D 选项说在交换机上把 IP 地址和 MAC 地址进行绑定，来阻止 IP 地址欺骗。这里首先要清楚在一台二层交换机上是无法完成把二层的 MAC 地址和三层的 IP 地址进行绑定的工作的，在三层交换机上才可以完成；其次，与题目的要求不符。F 选项说配置一个访问控制列表，拒绝服务器的 MAC 地址从 Fa0/1 以外的端口进入，这与题目的要求也不符。

6. 解：AD

题目问：网络安全策略要求仅允许一台主机被动态地连接到每一个交换机端口，如果违反了策略，接口将被关闭。网络管理员必须配置哪两个命令来满足这个策略（选两个）？“switchport port-security maximum 1”这个命令是配置只允许学习一个 MAC 地址；“switchport port-security violation shutdown”这个命令的意思是如果端口违反了安全策略，就 shutdown 该接口。

7. 解：BE

题目问，为了能通过 Telnet 连接到一台有适当安全要求的思科交换机，并能改变设备的配置，哪两个密码必须被提供？参照本章 9.3.3 节，可以得知，vty 密码和 enable 密码需要被配置。

第 10 章

VLAN***

本章从 VLAN 的由来讲起，介绍 VLAN 的优点、VLAN 干线、VLAN 的封装和工作方式、VLAN 的配置、VLAN 间路由的实现，以及 VLAN 的故障排除。



10.1 VLAN 介绍**

本节介绍 VLAN 的由来，以及 VLAN 的优点。

10.1.1 VLAN 的由来*

LAN (Local Area Network, 局域网) 的特征是所有结点都能互相直接通信，而不必通过某种第三层或更高层的设备，例如路由器。在大多数情况下，这些直接通信是通过向目标 IP 地址发送 ARP 广播请求报文，获取目的 IP 地址对应的 MAC 地址，然后用单播 MAC 地址实现相互通信。在传统的局域网中，如果一个结点接到一个网络设备，包括 Hub (集线器)、Repeater (中继器)、Bridge (网桥) 和 Switch (没有划分 VLAN 的交换机) 上，那么它就与其他接在同一设备上的结点属于同一个局域网 (这里局域网指的就是一个广播域)。在图 10-1-1 中，计算机 PCA 接在集线器 HubA 上。接在 HubA 上的任何其他第一层或第二层设备都是同一 LAN 的一部分，并且接在这些设备 (中继器、集线器、网桥、非 VLAN 型的二层交换机，图 10-1-1 中的 Bridge 和 HubB) 上的结点与接在 HubA 上的结点属于同一个 LAN。图 10-1-1 中的所有设备属于同一个 LAN。

说得抽象一些，局域网实际上就是一组能够互相发送广播报文的结点。如果一组结点能互相发送广播报文，就称它们处于同一个“广播域”。说得更明白一些，就是：广播域是一组能互相发送广播报文的结点。广播域通常通过路由器互相连接，并且第二层的广播帧不能通过路由器。

在图 10-1-2 中，有 4 台 PC 接在一台交换机上，其中，PC1 和 PC2 属于技术部，PC3 和 PC4 属于销售部。在默认情况下，4 台 PC 处在同一个 LAN 中，相互间都可以收到对方的广播报文。这样的网络管理难度大，经常发生 IP 地址冲突，网络病毒泛滥。以往解决的办法是网络的物理隔离，每个部门使用一台单独的交换机，两个交换机之间不做连接，也就是两个分开的 LAN。可这样也有缺陷，首先就是要购买第二台交换机；其次，如果两个部门的人员有人事变动，还要涉及重新布线的问题。要是能把一台交换机当成两台虚拟的交换机用就好了，两台虚拟交换机相互之间互不影响，并能动态地调整两台虚拟交换机的端口，这种技术就是本章要介绍的 VLAN (Virtual LAN, 虚拟局域网)。

通过在支持 VLAN 的交换机上添加 VLAN，并动态地调整每个端口所属的 VLAN，实

现一台物理的交换机上可以有多个 LAN，每一个 LAN 称为 VLAN，VLAN 之间的广播报文相互不可达，VLAN 间相互不影响。在一台 VLAN 型交换机上划分多少个 VLAN，交换机上就有多少个广播域，为了简单起见，称一个 VLAN 就是一个广播域。

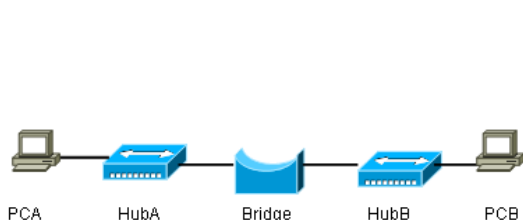


图 10-1-1 LAN 范围

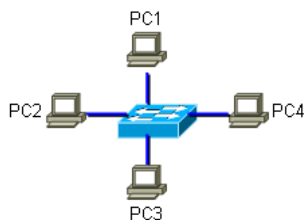


图 10-1-2 VLAN 交换机

虽然一个 VLAN 粗略等价于一个广播域，但 VLAN 型交换机并不等价于传统型的交换机。区别在于：传统型的交换机只包含一个广播域，而 VLAN 型交换机可以有多个。思科生产的所有交换机都支持 VLAN 功能，当然价格也相对较贵，一般都在几千元以上。国产交换机，价格相对便宜，一般价格在 1000 元以下的交换机都不支持网管，也不支持 VLAN 功能；价格在 1000 元以上的交换机基本都支持网管，也支持 VLAN 功能。

10.1.2 VLAN 的优点**

使用 VLAN 可以使网络更灵活地支持公司业务，进一步提高员工的工作效率，为公司带来效益。实施 VLAN 的主要好处有：

- Security（安全）

VLAN 能提高网络安全。如果网络划分为 VLAN，那么不同 VLAN 中的结点要想互相通信，必须通过一个三层以上（包括三层）的设备，比如三层交换机、路由器或者一个防火墙。在这种情况下，就可在三层设备上配置访问列表，使其阻止部分业务流在 VLAN 之间流动。由于业务流不能在一个交换机内的多个 VLAN 之间随意流动，安全绝对可靠。

- Cost reduction（降低开销）

考虑图 10-1-2 中的描述，如果交换机不支持 VLAN，为了隔离不同的部门就需要使用多台交换机，即使是两个人的部门也需要占用一台交换机；因为人员的频繁变动还涉及网络的重新布线。如果使用了 VLAN 技术，在交换机端口数量允许的情况下，所有的部门都可以接在一台交换机上，并可以调整每个交换机端口所属的 VLAN 来适应单位人事关系的变动，而不涉及重新布线。

VLAN 降低开销的同时，也提供了灵活性，不需要考虑用户所处的物理位置，只需要根据部门划分 VLAN 就可以了。

- Higher performance（高性能）

通过在第二层的网络中划分 VLAN，把一个大的广播域分隔成多个逻辑工作组（广播域），减少逻辑组之间不必要的广播流量，提升网络的性能。

- Broadcast storm mitigation（减轻广播风暴）

通过划分 VLAN，把一个大的广播域分隔成多个逻辑工作组，每个逻辑工作组中的计算机数量都不是很多，可以有效减小每个工作组中的广播。

- Improved IT staff efficiency（提高了 IT 员工效率）

VLAN 使 IT 部门更易于管理网络用户，因为相同部门的用户处在相同的 VLAN 中，有

着相同的需求。网络管理员可以为每个部门分配 IP 地址，制定策略，这样不仅有利于管理，也有利于网络故障排除。比如 VLAN 2 是学生所在的 VLAN，有一个学生发动了 ARP 攻击，影响的范围有限，只能是在学生 VLAN 中；排查简单，只需要排查学生 VLAN 就可以了。

- Simpler project or application management（简单的项目或应用管理）

不同的 VLAN 有不同的应用，可以很容易地根据每个部门部署应用程序。



10.2 VLAN 干线***

本节介绍什么是干线、干线协议、交换机间 VLAN 的通信过程等。

10.2.1 什么是干线**

VLAN 交换机的主要特点是能够在单个交换机内部或多个交换机之间支持多个独立的 VLAN。图 10-1-2 中介绍了在单个交换机内部存在多个 VLAN 的情况下，只需把交换机端口划分到特定的 VLAN 中即可实现端口之间的隔离。

下面开始讨论如何在交换机之间扩展 VLAN。在图 10-2-1 中，有两台交换机 SW1 和 SW2，PC1、PC2、PC3 和 PC4 分别连接在 SW1 和 SW2 上，其中，PC1 和 PC3 属于 VLAN 2，PC2 和 PC4 属于 VLAN 3。在不使用 Trunk（干线）的情况下，为了使 PC1 和 PC3 之间可以通信，需要在交换机 SW1 和 SW2 之间连接一条线缆，并把线缆连在 SW1 和 SW2 上的接口也划入 VLAN 2，这样 PC1 和 PC3 就可以跨交换机通信了。同理，为了使 PC2 和 PC4 之间可以通信，需要在交换机 SW1 和 SW2 之间再连接一条线缆，并把线缆连在 SW1 和 SW2 上的接口也划入 VLAN 3，这样 PC2 和 PC4 也可以跨交换机通信了。

从上面的叙述中可以发现，在不使用干线的情况下，若要使两台交换机之间的多个 VLAN 可以相互通信，需要在两台交换机间连多条线缆。通过这种方式实现 VLAN 跨交换机的通信，不仅浪费线缆，增加工程的难度和费用，还会造成交换机端口的浪费。可以通过在两台交换机间的一根线缆上传输多个 VLAN 的信息，这根线缆被称为主干（Trunk），主干上可以传输多个 VLAN 的信息，如图 10-2-2 所示。

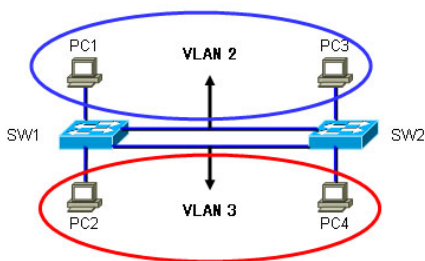


图 10-2-1 不使用干线的情况

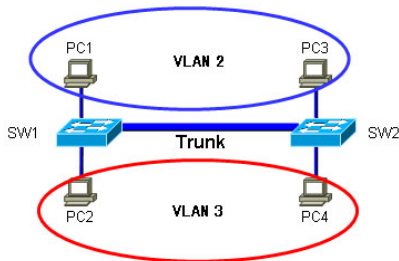


图 10-2-2 干线传输

从图 10-2-2 中，读者认识到了干线的作用，但读者不要误以为干线是一种特殊的线缆，干线也是普通的线缆，干线主要是体现在交换机端口的配置上，本章稍后介绍干线的配置。因为 10Mb/s 以太网和 100Mb/s 快速以太网在技术上有差异，且干线上需要传输多个 VLAN 的信息，10Mb/s 的链路显然难以胜任，思科没有针对 10Mb/s 链路再做开发，也就是说，只有 100Mb/s 以上（包括 100Mb/s）的链路才支持 Trunk。

10.2.2 干线协议**

对于 VLAN 交换机来说,干线就是交换机之间的连接,它可以在两个或两个以上的 VLAN 之间传输业务流。这与两个普通网桥之间的一条链路不同,因为每个交换机必须确定它所收到的数据帧属于哪个 VLAN。虽然这增加了某种复杂性,但同时也带来了很大的灵活性。考虑到图 10-2-2 中的两台交换机可能分布在两幢建筑物内,如果使用干线连接,两幢建筑物间只要有一条链路就可以了。一条干线上可以同时传输多个 VLAN 的信息,即使在两幢建筑物内新增 VLAN,建筑物间的连线也不需要做任何调整;如果使用的是图 10-2-1 中的方案,每次增加 VLAN,都需要在两幢建筑物间重新布线。

考虑一下传统型的交换机(非 VLAN 交换机)是如何知道一个帧要发往哪个目标端口的。当一个帧进入交换机时,交换机必须决定将其送往何处。传统型的交换机只简单地检查数据帧的目的 MAC 地址,再参照 MAC 地址表,然后将其转发到适当的端口,而不考虑数据帧是从哪儿来的。如果不知道目的地址,或者目的地址为广播地址,那么交换机就用“泛洪法”将其转发到除接收到此数据帧端口之外的所有端口。

在 VLAN 中,情况要稍复杂一些。除了要根据目的 MAC 地址做转发决定外,还必须考虑帧的源地址,因为帧的源地址通常会影响到它所属的 VLAN,并因此影响到它可能会被转发去的端口。追踪一个帧的源地址至少有两种显而易见的方法:第一种是根据数据帧进入的端口属于哪一个 VLAN,这种方法被称为“帧标记”,也称为“显式标记”。注意:这个过程只发生在交换机的内部。第二种追踪帧的源地址的方法是为每个 VLAN 保持一张 MAC 地址表(这张表由交换机通过某种方式完成)。确定目的地址后,就做出是否转发此帧的决定。这种方法称为“帧过滤”,也称为“隐式标记”。

“帧标记”和“帧过滤”的主要区别在于何时做出 VLAN 决定。在帧标记中,帧一进入交换机,决定就已经做出。在帧过滤中,当帧需要转发时才做出决定,帧刚进入交换机时,并不需要做出决定。对于交换机如何在其内部做出 VLAN 成员关系的决定,大多数讨论都是学术性的。事实上,交换机如何在其内部追踪 VLAN 并不重要,只要它能做出正确的转发决定就行。

帧标记的优点是能够立即标识 VLAN,并且不需要对帧做进一步的 VLAN 成员关系决定。标记过程是通过给帧增加一个包含 VLAN 标识的域来实现,Cisco 文档中有时将这个�程称为“VLAN 着色”(VLAN Coloring)。这种方法的缺点是大多数不支持 VLAN 的设备会把这种帧当成无效帧,因为它们没有遵照标准格式。同样,在帧标记方法中,由于众多设备生产厂商的存在,也带来很多不兼容性问题。为了解决不同厂商之间帧标记兼容性的问题,IEEE 组织定义了一个标准的帧标记机制,那就是 IEEE 802.1Q 标准,简称 802.1Q。

帧过滤的优点是不修改帧,因此,在帧通过任何网络设备时不会出现问题。缺点是所有 VLAN 设备必须能对每个帧做出唯一的 VLAN 决定。这意味着如果按数据帧中的源 MAC 地址进行过滤,那么所有 VLAN 交换机必须拥有一张 MAC 地址表,该表还要包含每个 MAC 地址所属的 VLAN。

事实上,帧标记多少占了点上风。所有主要的交换机厂商在他们的实现方案中都喜欢采用帧标记,IEEE 里的相关标准也是为帧标记制定的,传统的骨干网 FDDI(Fiber Distributed Data Interface,光纤分布式数据接口)支持帧标记,Cisco 支持两种帧标记,即 ISL(Interior Switching Link,交换机间链路)和 IEEE 802.1Q。只有 ATM LANE(LAN Emulation,局域

网仿真)是个例外,它与帧过滤更相似。

接下来介绍几种干线传输协议。Cisco 的 Catalyst 系列交换机支持 4 种干线传输协议:交换机间链路 (ISL)、802.10 (FDDI)、802.1Q, 以及局域网仿真 (LANE)。并不是所有的干线传输协议在每一种型号的 Catalyst 交换机上都能使用,例如 LANE 作为一种 ATM 协议,就不能在不支持 ATM 的低端交换机上使用。要想知道何种交换机支持何种干线传输协议,请参考交换机的相关参数文档。802.10 和 LANE 并不常用,本书仅针对最常使用的两种干线传输协议 ISL 和 802.1Q 进行讲解。

事实上,虽然思科交换机可以被配置来支持两种主干端口: ISL 和 802.1Q,但现在默认使用的是 802.1Q。然而在一些老的交换机中,默认使用的是 ISL。在不同厂商设备混用的情况下,一定要使用 802.1Q,对一些老的思科交换机,要改变主干端口的封装协议。

1. ISL

交换机间链路 (ISL) 是 Cisco 创建的私有干线传输协议。这里的“私有”是指该协议不是由一个独立的标准组织创建并通过的,但这不表示该协议在非 Cisco 产品中看不到。实际上多宿主服务器 (multihome server) 中就有一些网卡和驱动程序能够执行 ISL,有些交换机厂商也在他们的交换机产品中支持 ISL。

ISL 能支持多种不同大小的帧。ISL 头占用 26 个字节,当干线传输数据帧时,这 26 个字节也要加到帧里。同时,在帧尾还要加上一个 4 个字节的新的 CRC (循环冗余校验) 校验码,这种为帧增加一个新头与校验和的过程称为封装。ISL 封装整个帧,而不做任何分割工作。

ISL 帧头中有 10 个 bit 被用来标识 VLAN,能够表示 1024 个 VLAN,编号从 0 到 1023,其中有很多号是保留的。因此,有些 Cisco 文档中称可用的 VLAN 号是 1000 个。

2. 802.1Q

802.1Q 出现之前,很多厂商都声称他们的交换机实现了 VLAN,但各个厂商实现的方法都不相同,所以彼此间无法互连,这样,用户一旦买了某个厂商的交换机,就没法再买其他厂商的交换机了。而现在,VLAN 的标准是 IEEE 提出的 802.1Q 标准,是一个通用标准。802.1Q 的帧是在原来的以太网帧头中的源地址后增加了一个 4 个字节的 802.1Q 帧头,添加新的字段域后,帧被重新计算 FCS (Frame Check Sequence, 帧校验序列),用新的 FCS 替换原来帧中的 FCS,其他字段保持不变。修改前后的帧如图 10-2-3 所示。

新增标签头中的 4 个字节信息如下:

- 网络类型: 2 个字节的标签协议标识,以太网帧的值是 0x8100。
- VLAN 标识: 这是一个 12 位的域,指明 VLAN 的 ID,最大可以支持 4096 个 VLAN,每个 802.1Q 的帧都会包含这个域,以指明帧属于哪一个 VLAN。
- 令牌环标记: 这 1 位主要使总线型的以太网与 FDDI、令牌环网交换数据时更容易。
- 优先级: 这 3 位指明帧的优先级,被用于 QoS,一共有 8 种优先级,主要用于当交换机阻塞时,优先发送哪些数据帧。

10.2.3 交换机间 VLAN 的通信过程***

接下来看一下 VLAN 交换机的工作方式。因为 802.1Q 是一个标准协议,使用面广,在工程和 CCNA 考试中,802.1Q 都是重点,对 ISL 有一个了解就可以了,接下来的分析

和配置均以 802.1Q 为例。在图 10-2-4 中, PC1、PC3 属于 VLAN 2, PC2 和 PC4 属于 VLAN 3。

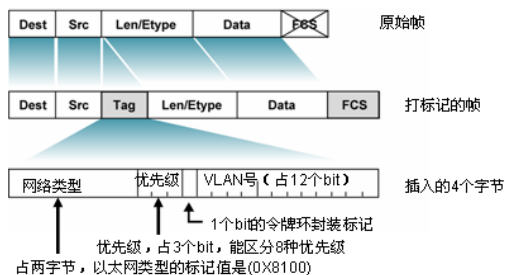


图 10-2-3 802.1Q 的帧格式

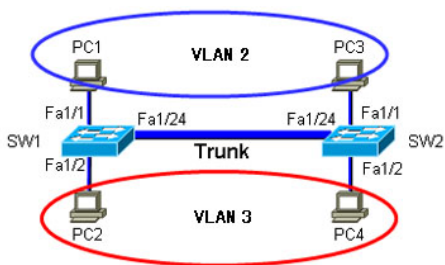


图 10-2-4 交换机间的 VLAN 通信

假设 PC1 要发送一个数据包给 PC3, 刚开始时 PC1 并不知道 PC3 的 MAC 地址, 为了完成数据包的发送, PC1 首先发送一个 ARP 查询包, ARP 查询包以广播的形式发送。

交换机 SW1 收到了 PC1 发过来的 ARP 广播包, SW1 知道该数据包是从 Fa1/1 接口接收到的, Fa1/1 接口被分配到了 VLAN 2 中, 是一个 Access (接入) 端口, SW1 知道这是一个来自 VLAN 2 的广播包, SW1 在 MAC 地址表中加入 PC1 的 MAC 地址和对应的 VLAN 号及端口号, VLAN 交换机与非 VLAN 交换机都会根据数据帧的源 MAC 地址进行学习, 只不过 VLAN 交换机除了记录 MAC 地址对应的端口外, 还要记录 MAC 地址对应的 VLAN 号。SW1 在数据帧中加入 VLAN 2 的标识, VLAN 交换机从 Access 端口接收到数据帧时, 需要插入 VLAN 标识。SW1 把 ARP 广播包从除 Fa1/1 之外所有属于 VLAN 2 的端口发送出去, 发送出去之前, 交换机要去除数据帧中被加入的 VLAN 2 标识, VLAN 交换机从 Access 端口发出数据帧之前, 要去除 VLAN 标识, 不然其他计算机收到这样不符合标准的数据帧, 将会因为不能识别而把数据帧丢弃。交换机除了把广播帧从所有属于 VLAN 2 的端口发送出去之外, 还要从所有的主干端口把广播帧发送出去, 也就是要从 Fa1/24 端口发送出去。当交换机从主干端口转发数据帧时, 不修改数据帧的格式 (下一节介绍的 Native VLAN 除外), 也就是说, SW1 发往 SW2 的 ARP 广播帧中, SW1 加入的 VLAN 标识不会被清除掉。

这里要知道 PC2 接收不到 PC1 发出的广播帧, 因为 PC1 和 PC2 分属于不同的 VLAN, 不同的 VLAN 是不同的广播域, 交换机不会把一个 VLAN 中的广播转发到另一个 VLAN 中。

当 SW2 从 Fa1/24 端口 (主干端口) 收到一个数据帧时, SW2 查看数据帧中的 VLAN 标识, 并在 MAC 地址表中添加学到的 MAC 地址和对应的 VLAN 号及端口号。SW2 接下来要决定向哪里转发数据帧, SW2 查看数据帧中的 VLAN 标识, 知道是 VLAN 2 的数据帧, SW2 查看数据帧的目的 MAC 地址, 知道这是 VLAN 2 的一个广播帧。SW2 把广播包从除 Fa1/24 之外所有属于 VLAN 2 的端口发送出去, 发送出去之前, 交换机要去除数据帧中被加入的 VLAN 2 标识。

PC4 是收不到这个数据帧的。

PC3 收到这个数据帧后, 知道是 PC1 发给自己的 ARP 请求帧。PC3 封装 ARP 应答包, 把应答包发往交换机 SW2。

当 SW2 从 Fa1/1 (Access 端口) 收到一个数据帧时, SW2 在 MAC 地址表中添加 MAC 地址和对应的 VLAN 号及端口号。SW2 在数据帧中添加该端口所在的 VLAN 标识。SW2 查询 MAC 地址表, 找到 PC1 对应的 MAC 地址、VLAN 号和端口号, SW2 比较数据帧的

源 MAC 地址和目的 MAC 地址在同一个 VLAN 中, SW2 把数据帧从数据帧目的 MAC 地址对应的端口 Fa1/24 发往 SW1。

当 SW1 从主干端口收到一个数据帧时, SW1 首先也是学习 MAC 地址和对应的端口号及 VLAN 号。SW1 然后查询数据帧中的目的 MAC 地址, 之前已经保存过 PC1 的 MAC 地址, SW1 比较数据帧中源和目的 MAC 地址在同一个 VLAN 中。SW1 去除 VLAN 标识, 把数据帧从 Fa1/1 端口发往 PC1。

PC1 成功接收了 PC3 的 ARP 应答包。接下来的通信过程与 ARP 的解析过程类似。

至于交换机何时添加或删除 802.1Q 标签头, 与交换机的端口有关系, 如果交换机的端口接的是一台计算机, 那么该端口属于接入端口 (Access), 数据帧进入时被添加 802.1Q 标签头, 数据帧从接入端口发出时被移除 802.1Q 标签头; 如果交换机的端口接的是另一台交换机, 那么该端口属于主干端口 (Trunk), 一般 802.1Q 标签头不会被改变, 特殊情况除外 (Trunk 端口会添加或移除该端口 Native VLAN 的 802.1Q 标签头, 有关这一点, 下一节进行演示)。

10.2.4 DTP 协议***

DTP (Dynamic Trunking Protocol, 动态主干协议) 是思科公司私有的协议, 其他厂商的交换机不支持 DTP。当思科交换机端口被配置成某些主干模式时, DTP 被自动运行, 用来协商链路能否成为主干链路。DTP 既支持 ISL 封装的主干链路协商, 也支持 802.1Q 封装的主干链路协商。

思科交换机端口支持多种主干模式。主干模式定义了端口如何与对端端口使用 DTP 协商来建立主干链路, 下面是思科交换机端口的几种主干模式。

- OFF (关闭)

使用 “switchport mode access” 命令, 静态配置交换机端口为接入端口 (非主干端口)。当交换机端口被静态配置成非主干端口时, 该端口不向外发送 DTP 消息, 并忽略远端发过来的 DTP 消息, 该端口无条件地被配置成接入端口。

- ON (打开)

使用 “switchport mode trunk” 命令, 静态配置交换机端口的主干模式。当交换机端口被静态配置成主干模式时, 该端口定期向外发送 DTP 消息, 通告远端的端口, 希望对方端口改变成主干状态。如果交换机的端口被静态配置成主干端口, 该端口将忽略远端发过来的 DTP 消息, 该端口无条件地被配置成主干模式。

- Dynamic auto (动态自动)

使用 “switchport mode dynamic auto” 命令, 配置交换机端口的主干模式为动态自动模式。配置为动态自动的端口能够成为主干, 但不会主动转换到主干模式, 这样的端口不主动发送 DTP 消息, 被动地等待对方的协商。如果远端交换机端口被配置成 ON 或 Dynamic desirable, 则链路可以协商成主干链路。如果远端交换机被配置成 OFF 或 Dynamic auto 时, 则动态链路协商失败。

- Dynamic desirable (动态期望)

使用 “switchport mode dynamic desirable” 命令, 配置交换机端口的主干模式为动态期望模式。当交换机端口被配置成动态期望模式时, 该端口定期向外发送 DTP 消息, 通告远端的端口自己可以转变到主干状态, 并要求远端也改变到主干状态。如果远端交换机的端口被配置成主干 ON、Dynamic auto、Dynamic desirable, 则链路协商成主干链路。如果远端

交换机的端口被使用“switchport nonegotiate”命令关闭 DTP 协商，则链路主干协商失败，链路仍然是非主干链路。

• Nonegotiate（关闭 DTP 协议）

使用“switchport nonegotiate”命令关闭 DTP 协议。当两端交换机的端口都被静态配置成主干链路时；或一端是思科的交换机，另一端是非思科的交换机时，则可以考虑关闭 DTP 协议，节省带宽。

交换机的端口可支持上述 5 种模式，在什么情况下能建立起主干链路，在什么情况下建立不起主干链路，在什么情况下是失败的链路，表 10-2-1 列出了各种可能的组合。

表 10-2-1 主干链路协商表

	OFF	ON	ON and Nonegotiate	Dynamic auto	Dynamic desirable
OFF	Access	错误	错误	Access	Access
ON	错误	Trunking	Trunking	Trunking	Trunking
ON and Nonegotiate	错误	Trunking	Trunking	错误	错误
Dynamic auto	Access	Trunking	错误	Access	Trunking
Dynamic desirable	Access	Trunking	错误	Trunking	Trunking

注：Access 是指链路协商后，最后成为非主干链路；Trunking 是指链路协商后，最后成为主干链路；错误是指有故障的链路，一端设成了主干，另一端是非主干，两端的认识达不成一致，跨交换机的 VLAN 通信失败。

为了读者更好地理解，这里想象成两个未婚的青年男女，协商最后能否走进婚姻殿堂。OFF 相当于谁都不爱（非主干端口），ON 相当于告诉对方自己非她不娶；ON and Nonegotiate 相当于非对方不娶但没有告诉对方，可以理解成暗恋；Dynamic auto 相当于爱对方，但不会主动表达；Dynamic desirable 相当于爱对方，并愿意主动告诉对方。Access 表示结不了婚，Trunking 表示结成了婚，错误表示有人受到了伤害。这样再来理解表 10-2-1 就很好理解了，对照表的第二行，两个谁都不爱的人碰到一起，结果自然是结不成婚；一个谁都不爱的人和一个爱得发疯的人，结果只能说是一种错误；一个谁都不爱的人和一个爱得发疯、却没有表达出来的人也是一种错误，够痴呆的；一个谁都不爱的人和一个爱对方的人碰到一起，碰不出火花，也不存在大的伤害；一个谁都不爱的人和一个爱对方并主动表达了爱意的人碰到一起，碰不出火花，也不存在大的伤害。

Dynamic auto 碰到 Dynamic auto 是什么情况呢？两个都爱对方的人，碰到了一起，可没有一个人主动表达爱意，结果只能是错失良机，还是结不了婚。Dynamic auto 如果碰到了 Dynamic desirable 就不一样了，一个爱对方，但不愿主动表达，另一个也爱对方，并主动表达，结果结婚了。ON and Nonegotiate 碰到了 Dynamic desirable 会出现什么情况呢？Number ONE 深爱着对方，但比较害羞，爱却不愿说出口，Number TWO 也很爱 Number ONE，并主动表达了爱意，可 Number ONE 害羞，没有给出任何表示，Number TWO 一气之下出家为僧，Number ONE 仍然痴爱着 Number TWO，结果自然是一种伤害。ON and Nonegotiate 碰到了 ON and Nonegotiate 的情况是，爱都不说出来，直接结婚，这种方式是最受欢迎的方式，省得一来二去，白浪费时间（带宽）。



10.3 配置 VLAN***

本节介绍配置 VLAN、配置 Trunk、配置语音 VLAN、配置本地 VLAN，最后是 VLAN

的实验和测试。

10.3.1 配置单台交换机上的 VLAN***

交换机端口的 VLAN 划分有静态和动态之分：

(1) 静态 VLAN

静态 VLAN 很容易理解，因此先讨论它。静态 VLAN 由其所处的机架特征定义，通常包括插槽、端口或端口组等。例如，在一个有 16 个端口的交换机上，1~8 号端口可以属于 1 号 VLAN，9~16 号端口可以属于 2 号 VLAN。

(2) 动态 VLAN

动态 VLAN 通常由接到机架上的结点的某些特征定义。这可以是结点的 MAC 地址、正在使用的协议，甚至是某些认证信息，如名字与口令等。CCNA 中不涉及动态 VLAN 的配置。

在 Packet Tracer 模拟器中设计如图 10-3-1 所示的网络拓扑，然后基于此拓扑，在 Packet Tracer 中完成本节的相关实验。

在 Packet Tracer 中绘制的模拟拓扑如图 10-3-2 所示，图中使用了 1 台集线器、2 台 2960 的交换机、5 台 PC。图中使用了 5 根直通的双绞线、2 根交叉的双绞线，所有线缆使用均正确，因为图中的每一根线缆都有绿色标记，表示链路正常；如果有红色标记，则表示链路不正常；有些链路是橙色标记，稍后会变成绿色标记，至于为何会出现这种情况，本书第 12 章 STP 中有介绍。读者可自行绘制这样的拓扑，也可以在 Packet Tracer 中直接打开光盘中的“配置\10\vlan.pkt”文件，调入图 10-3-2 中的拓扑。Packet Tracer 中设备的编号都是从 0 开始的，如 PC0、PC1、PC2，读者只需要删除 PC0 就可以了，其他设备也类似地添加，这里从 1 开始，仅仅是一种习惯，设备的外观名字并不影响设备的配置。

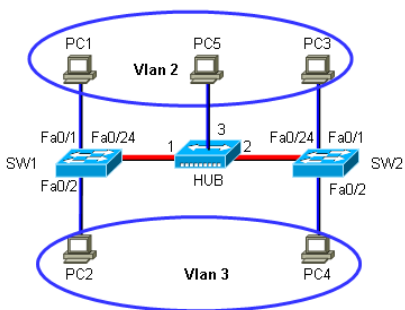


图 10-3-1 VLAN 拓扑

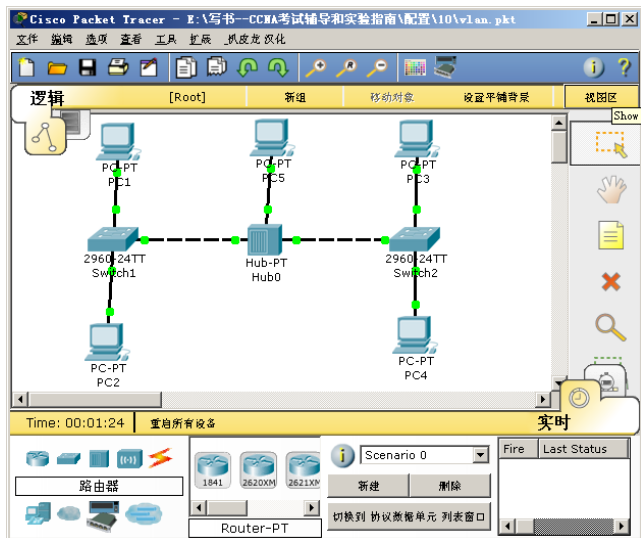


图 10-3-2 Packet Tracer 中的模拟拓扑

单击如图 10-3-2 所示工作区域中的 PC1，打开如图 10-3-3 所示的 PC 配置界面。从图中可以看到 PC 还支持一些模块类型，比如无线网卡、千兆位以太网网卡、ATM 网卡等。PC 上只提供了一个插槽，单击图 10-3-3 中的“放大”按钮，对 PC 的图像进行缩小，可以在

PC 的最下面看见默认配置的快速以太网网卡。如果需要使用其他网卡，只能是更换，断开 PC 的电源，把 PC 上已经安装的模块拖放到模块区，从模块区重新再拖一块模块放入 PC 的插槽，然后给 PC 加电。本实验中不需要更换 PC 的网卡。

单击图 10-3-3 中的“桌面”标签，打开 PC1 的桌面，如图 10-3-4 所示。从图中可以看出模拟 PC 的功能还是挺强的，支持 IP 配置、拨号、超级终端、DOS 命令行、Web 浏览器、无线和 VPN 等。



图 10-3-3 PC 配置界面



图 10-3-4 PC1 的桌面

单击图 10-3-4 中的“IP 配置”图标，配置 PC1 的 IP 地址为 192.168.1.1/24，网关和 DNS 暂且不配。类似地，配置 PC2 的 IP 地址为 192.168.1.2/24，PC3 的 IP 地址为 192.168.1.3/24，PC4 的 IP 地址为 192.168.1.4/24，PC5 的 IP 地址为 192.168.1.5/24。都配置完成后，单击图 10-3-4 中的“Command Prompt”图标，打开 PC1 的 DOS 命令行窗口，分别 ping PC2、PC3、PC4、PC5 的 IP 地址，如图 10-3-5 所示，都可以 ping 通。

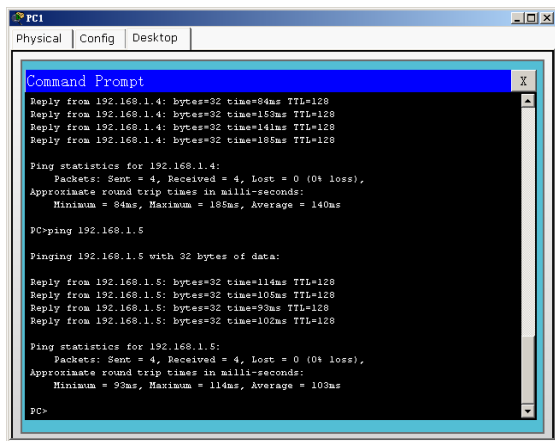


图 10-3-5 PC 的 DOS 命令行

PC 配置完成后，接下来配置交换机。单独的一台交换机上配置 VLAN 一般分成两个步骤。

步骤一：创建 VLAN。

单击如图 10-3-2 所示工作区域中的 Switch1，打开如图 10-3-6 所示的交换机配置窗口。

从图中可以看出 2960 没有模块可供选择, 有 26 个水晶头接口, 和真实设备一样, 交换机上没有电源开关。

单击图 10-3-6 中的“命令行”标签, 进入交换机的命令行配置窗口, 使用“show ip int brief”命令查看交换机上有哪些端口, 显示如图 10-3-7 所示。

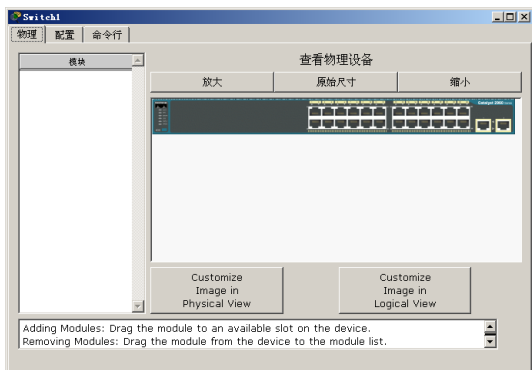


图 10-3-6 交换机配置窗口



图 10-3-7 交换机的 CLI 界面

从如图 10-3-7 所示的输出中, 可以看到 2960 交换机配备了 24 个快速以太网接口和 2 个吉比特以太网接口。在交换机上创建 VLAN 有两种方式: 一种是全局配置模式, 思科推荐使用这种配置模式, CCNA 考试中仅要求掌握这种配置模式; 另一种是 VLAN 数据库配置模式, 很多老的工程师都习惯使用这种模式, 思科有可能在将来的交换机上不再支持这种配置模式。为了演示这两种配置模式有何不同, 在 SW1 上使用全局配置模式, 在 SW2 上使用 VLAN 数据库配置模式。SW1 的配置如下:

```
Switch>en
Switch#conf t
Switch(config)#host SW1
SW1(config)#vlan 2
SW1(config-vlan)#name student
SW1(config-vlan)#vlan 3
SW1(config-vlan)#name teacher
```

新增 VLAN 2, 模拟器上最大能配置的 VLAN 号是 1001。
VLAN 2 的名字是 student, 看起来更直观。
不用退回到全局配置模式, 新增 VLAN 3。
VLAN 3 的名字是 teacher。

配置完成后, 在 SW1 上使用“show vlan”或“show vlan brief”命令查看 VLAN 的信息, 关键部分显示如下:

```
SW1#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
2	student	active	
3	teacher	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

从上面的输出中, 可以看到 SW1 上已经存在了 7 个 VLAN, 1002~1005 这 4 个是固定

存在的 VLAN，用不到也不用理会。VLAN 1 是交换机上默认存在的 VLAN，VLAN 1 不能删除也不能改名字，在默认情况下，交换机上的所有端口都属于 VLAN 1。VLAN 2 是刚才新增的 VLAN，名字叫 student，没有端口属于 VLAN 2，也没有端口属于 VLAN 3。再次进入 VLAN，使用 name 命令可以给 VLAN 重新命名。在全局配置模式下，使用“no vlan vlan 的编号”，可以删除对应的 VLAN。

SW2 的配置如下：

```
Switch>en
Switch#vlan database          进入 VLAN 数据库配置模式。
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.
提示不推荐使用这种模式配置 VLAN，建议使用全局配置模式，这里不用理会。

Switch(vlan)#vlan 2 name student      新增 VLAN 2，并直接命名。
VLAN 2 added:                          提示 VLAN 2 被添加了。
    Name: student    VLAN 2 的名字是 student，如果不给 VLAN 起名字，默认的名字是 VLAN0002。
Switch(vlan)#vlan 3 name teacher
VLAN 3 added:
    Name: teacher
Switch(vlan)#exit                退出 VLAN 配置模式。
APPLY completed.                应用改变。
Exiting...
```

至此，添加的 VLAN 才生效。如果是在真实的交换机上，还可以使用 abort 放弃更改退出，前面创建的 VLAN 不会生效。

配置完成后，在 SW2 使用“show vlan”或“show vlan brief”命令查看 VLAN 的信息，显示的内容与 SW1 上显示的内容相似。

步骤二：把端口加入 VLAN。

SW1 的配置如下：

```
SW1(config)#int fa 0/1          进入交换机的端口配置模式。
SW1(config-if)#switchport mode access
把端口的模式改成 Access，即接入端口，直接连 PC 或终端设备的端口。如果不改变端口的模式，这一款交换机默认的端口模式是 Dynamic auto，尽管最后协商的结果也是 Access，但存在安全隐患，譬如攻击者把连接的计算机换成交换机，并配置交换机端口为 Trunk，因为 DTP 的缘故，协商后，这台链路将成为主干链路，攻击者在私自架设的交换机上可以配置任何 VLAN，从而发动对任何 VLAN 的攻击。稍后演示如何查看端口的模式。
SW1(config-if)#switchport access vlan 2    把这个接入模式的交换机端口分配到 VLAN 2 中。
SW1(config-if)#int fa 0/2
SW1(config-if)#swi mo acc              命令被简写。
SW1(config-if)#swi acc vlan 3
```

配置完成后，在 SW1 上查看 VLAN 的信息，显示如下：

```
SW1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig1/1, Gig1/2
2	student	active	Fa0/1
3	teacher	active	Fa0/2

从上面的输出中，可以看到 Fa0/1 被分配到 VLAN 2 中，Fa0/2 被分配到 VLAN 3 中。

SW2 的配置如下：


```
SW2(config)#int fa 0/1
SW2(config-if)#swi mode acc
SW2(config-if)#swi acc vlan 2
SW2(config-if)#int fa 0/2
SW2(config-if)#swi mode acc
SW2(config-if)#swi acc vlan 3
```

配置完成后，在 SW2 上查看 VLAN 的信息，与 SW1 显示的类似，这里就省去输出了。

测试

交换机 SW1 和 SW2 的 VLAN 配置完成后，打开 PC1 的 DOS 命令行窗口，分别 ping PC2、PC3、PC4、PC5 的 IP 地址，结果一个也 ping 不通。

PC1 ping 不通 PC2，是因为它们虽然在同一台交换机上，但属于不同的 VLAN，所以无法 ping 通。

PC1 ping 不通 PC3、PC4、PC5，是因为 SW1 与集线器相连的端口 Fa0/24 是一个接入端口，该端口默认属于 VLAN 1，只能转发 VLAN 1 的数据包，而 PC1 在 VLAN2 中，所以都 ping 不通。下面介绍如何配置交换机上的主干链路，使 VLAN 可以跨交换机进行通信。

10.3.2 配置 Trunk***

(1) 配置主干端口

配置 SW1 的 Fa0/24 端口为主干模式，配置命令如下：

```
SW1(config)#int fa 0/24
SW1(config-if)#switchport mode trunk           配置交换机的端口为主干模式。
SW1(config-if)#switchport nonegotiate
关闭 DTP 协议，因为两端的端口都直接配置了 Trunk 模式，不需要再发送 DTP 包协商 Trunk 链路，这样可以节省带宽。
```

思科 2960 交换机主干链路的默认封装协议是 802.1Q，并且不再支持 ISL 封装协议。下面的命令在思科 2960 交换机上已经不被支持，但有一些老的思科交换机，默认的封装协议是 ISL。如果主干链路两端的封装协议不一致，将导致主干链路失败，使用下面的命令改变主干端口的封装协议，模拟器中不支持该命令。

```
Switch(config-if)#switchport trunk encapsulation ?
dot1q  Interface uses only 802.1q trunking encapsulation when trunking
isl    Interface uses only ISL trunking encapsulation when trunking
negotiate Device will negotiate trunking encapsulation with peer on
        interface
Switch(config-if)#switchport trunk encapsulation dot1q
```

从上面的输出中，可以看到该交换机支持 dot1Q（也就是 802.1Q）、ISL 或者自动协商封装协议。使用“switchport trunk encapsulation dot1q”命令把端口的封装协议改成 802.1Q。

配置 SW2 的 Fa0/24 端口为主干模式，配置命令如下：

```
SW2(config)#int fa 0/24
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport nonegotiate
```

(2) 配置主干端口允许传输的 VLAN

使用“switchport trunk allowed vlan”命令添加、删除、修改主干端口允许传输的 VLAN 信息。命令显示如下：

```
Switch(config-if)#switchport trunk allowed vlan ?
WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
add      add VLANs to the current list
all      all VLANs
```

```
except all VLANs except the following
none no VLANs
remove remove VLANs from the current list
```

WORD 是 VLAN 的列表，如果允许传输 VLAN 1、3、5、6、7、8、9、10，则可以写成：

```
Switch(config-if)#switchport trunk allowed vlan 1,3,5-10
```

如果想追加新的 VLAN，则可以写成：

```
Switch(config-if)#switchport trunk allowed vlan add 2
```

All、except、none、remove 参数的使用也比较简单，这里不做介绍。

(3) 查看主干链路状态

在 SW1 上查看主干链路端口的状态，显示如下：

```
SW1#show int fa 0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

下面的输出省略。

这个端口是交换端口。
配置的端口模式是 Trunk。
链路的状态是主干。
主干配置的是 dot1Q 封装。
有效的封装是 dot1Q。
主干协商关闭，也就是不使用 DTP 协议。
端口默认的 VLAN 是 1。
该主干端口的本地 VLAN 是 1。
没有配置语音 VLAN。

在 SW1 上使用“show interface trunk”命令显示交换机工作在主干模式的端口，显示如下：

```
SW1#show int trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/24    on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/24    1-1005

Port      Vlans allowed and active in management domain
Fa0/24    1,1002,1003,1004,1005

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/24    1,1002,1003,1004,1005
```

从上面的输出中，可以看出 SW1 的 Fa0/24 口 Trunk 的模式是 ON，802.1Q 的封装，工作模式是 Trunking，本地 VLAN 是 1。

在 SW2 上查看主干链路的端口状态和主干端口，显示的与 SW1 类似。

感兴趣的读者可以配置两边端口的各种主干模式，测试表 10-2-1 的正确性。比如把两边都配置成 Dynamic auto，显示如下：

```
SW1#show int fa 0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

配置的端口模式是 Dynamic auto。
链路的状态是非主干。
主干配置的是 dot1Q 封装。
有效的封装是 Native，因为主干链路没有协商成功，不使用 dot1Q 封装。
主干协商打开，也就是使用 DTP 协议。

使用“show interface trunk”命令显示交换机工作在主干模式的端口，显示如下：

```
SW1#show interfaces trunk
```

```
SW1#
```

显示没有任何端口工作在主干模式，即 SW1 和 SW2 的主干模式协商失败。

注意：改变端口模式时，要等待一会儿再查看主干链路协商结果，因为 DTP 协议的发送周期是 30 秒。有时可能需要保存交换机的配置，重启交换机后再查看主干链路协商的结果。

(4) 测试

在 PC1 上测试到 PC2、PC3、PC4、PC5 的连通性，结果是 PC1 只能成功地 ping 通 PC3。PC1 不能 ping 通 PC2 和 PC4 可以理解，也属于正常情况，因为它们属于不同的 VLAN，应该是 ping 不通的。可是 PC1 为何 ping 不通 PC5 呢？这就需要介绍 802.1Q 的本地 VLAN 技术了。

10.3.3 本地 VLAN**

本地（Native）VLAN 是主干端口的特征。使用 802.1Q 封装协议的主干端口，把数据帧从主干端口发出时，如果数据帧中的 VLAN 标识与主干端口的本地 VLAN 号相同，交换机清除数据帧中的 VLAN 标识。使用 802.1Q 封装协议的主干端口，从主干端口接收到数据帧时，如果数据帧中没有 VLAN 标识，交换机将在数据帧中添加主干端口的本地 VLAN 号。

下面分析在前面的测试中，为何 PC1 不能 ping 通 PC5？PC1 属于 VLAN 2，当 PC1 要发数据包给 PC5 时，需要先获取到 PC5 的 MAC 地址。PC1 查询 PC5 的 MAC 地址，ARP 请求包被以广播的形式发送出去。交换机 SW1 在广播帧上添加 VLAN 标识，然后从 Fa0/24 端口发出，Fa0/24 是主干端口，该主干端口的本地 VLAN 是默认的 1，主干端口的本地 VLAN 和数据帧中的 VLAN 标识不一样，交换机不修改该数据帧，把数据帧发出。Hub0 接收到这个数据帧，Hub 是物理层的设备，并不能识别帧，只是简单地把信号放大，然后从除接收端口以外的端口把比特流广播出去。PC5 收到了 PC1 发过来的 ARP 广播请求，但因为该 ARP 请求包中的数据帧格式已经被改变，被 SW1 添加了 802.1Q 封装，PC5 不能识别这样的数据帧，把 PC1 发过来的 ARP 请求包丢弃。PC1 获取不到 PC5 的 MAC 地址，无法完成数据包的封装，也无法与 PC5 进行通信。

使用下面的命令修改 SW1 主干端口的本地 VLAN。命令如下：

```
SW1(config)#int fa 0/24
```

```
SW1(config-if)#switchport trunk native vlan 2
```

把主干端口的本地 VLAN 修改成 VLAN 2，默认的本地 VLAN 是 VLAN 1。

主干链路两端交换机端口的本地 VLAN 要相同。如果两端交换机主干端口的本地 VLAN 不匹配，CDP 会提示“%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/24 (1), with SW1 FastEthernet0/24 (2).”的报错信息。使用下面的命令修改 SW2 主干端口的本地 VLAN：

```
SW2(config)#intfa 0/24
```

```
SW2(config-if)#switchport trunk native vlan 2
```

修改完成后，再次查看主干端口的交换特性，显示如下：

```
SW1#show int fa 0/24 switchport
```

```
Name: Fa0/24
```

```
Switchport: Enabled
```

```
Administrative Mode: trunk
```

```
Operational Mode: trunk
```

```

Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 2 (student)
Voice VLAN: none

```

注意到本地 VLAN 已经更换成 2 了。

在 PC1 上再次测试到 PC5 的连通性，结果可以 ping 通了。这是因为 SW1 从 Fa0/24 端口把数据帧发出时，当数据帧中的 VLAN 标识与主干端口的本地 VLAN 号相同时，交换机清除数据帧中的 VLAN 标识。Hub0 接收到不包含 VLAN 标识的数据帧，Hub0 把数据帧从端口 2 和 3 广播出去。PC5 收到数据帧，并可以识别标准的数据帧格式，PC5 对 PC1 发出的数据帧进行应答。PC5 发出的数据帧到达 Hub0，Hub0 把数据帧从端口 1 和 2 广播出去。SW1 从主干端口 Fa0/24 收到 Hub0 转发过来的数据帧，因为该数据帧中没有携带 VLAN 标识，SW1 认为这个数据帧是来自本地 VLAN——即 VLAN 2 的数据帧，SW1 给该数据帧添加 VLAN 2 的 VLAN 标识。SW1 查找 MAC 地址表和对应的 VLAN 号，知道该数据帧应该从 Fa0/1 发出，Fa0/1 是一个接入端口，SW1 清除数据帧中的 VLAN 标识，然后把数据帧从 Fa0/1 发出。PC1 和 PC5 可以正常通信，ping 测试成功。

10.3.4 语音 VLAN*

试想一下，正在接听一个紧急的 IP 语音电话，而单位突然有大量的邮件在发送，VoIP（Voice over IP，IP 电话）传输的质量严重下降，声音断断续续，甚至不能明白对方说什么。语音通信是实时通信，有它的特殊性，需要：

- 带宽保证，以确保语音质量。
- 优先传输，优于其他类型的网络流量。
- 拥塞避免，语音通信要提供拥塞避免功能。
- 延迟敏感，要求穿越整个网络的延迟小于 150 毫秒。

思科的 IP 电话机一般有两个接口：PC 接口和 Switch 接口。Switch 接口用来连接至交换机，PC 接口用来连接至计算机。IP 电话机可以单独连接在交换机上，有时为了节省交换机端口，也可以连接 IP 电话机后再连接普通计算机。

在 Packet Tracer 中，打开光盘中的“配置\10\vlan.pkt”文件，删除 PC1 和 Switch1 之间的以太网线，从“End Devices”设备列表中，拖入 IPPhone（IP 电话机）。拖入一根直连或交叉的双绞线连接 IP 电话机的 Switch 接口和 Switch1 的 Fa0/1 接口，然后再拖入一根直连的双绞线连接 IP 电话机的 PC 接口和 PC1 的以太网接口，如图 10-3-8 所示。

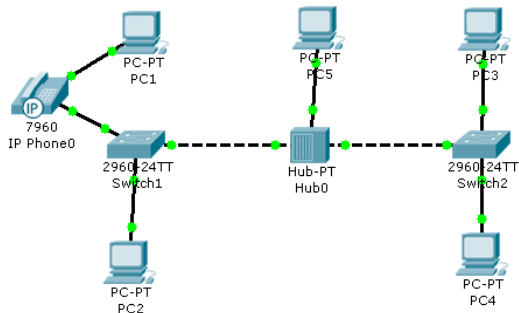


图 10-3-8 VoIP 拓扑

这里仅简单介绍 VoIP 的配置，有关语音 VLAN 的更多知识已超出 CCNA 的要求。Switch1 的配置如下：

```
SW1(config)#int fa 0/1
SW1(config-if)#swi mode acc
SW1(config-if)#swi acc vlan 2
SW1(config-if)#switchport voice vlan 50
```

Cisco IP 电话机有一个用于连接 PC 的接口，因此很多配置中都让 Cisco IP 电话机再串联一台 PC 计算机。由于 Cisco IP 电话机和工作站连接的是同一个交换机接口，因此将该接口加入 VLAN 中后，相应的 Cisco IP 电话机和工作站将位于同一个 VLAN 中。Cisco 交换机支持一种独特的功能，这种功能在 Cisco IOS 中被称为语音 VLAN，它将 Cisco IP 电话机和工作站加入不同的 VLAN 中。通过使用语音 VLAN，可将接口的 VoIP 通信流加入另一个 VLAN 中。如果希望使用语音 VLAN，那么只需要配置交换机，而无须在 Cisco IP 电话上做额外的配置。这里的语音 VLAN 是 VLAN 50。

在 SW1 交换机上可以查看语音 VLAN 的配置，显示如下：

```
Switch#show int fa 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 2 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

从上面的显示中可以看到“Voice VLAN: none”，这是 Packet Tracer 模拟器的问题，如果是在真实的思科交换机上，这里会显示成“Voice VLAN: 50”。

10.3.5 维护 VLAN 信息**

经过前面的配置后，使用“show run”命令查看交换机 SW1 的运行配置文件，显示如下：

```
SW1#show run
Building configuration...

Current configuration : 1127 bytes
!
version 12.2
no service password-encryption
!
hostname SW1
!
!
!
interface FastEthernet0/1
switchport access vlan 2
switchport mode access
switchport voice vlan 50
!
interface FastEthernet0/2
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
```

```

interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
  switchport trunk native vlan 2
  switchport mode trunk
  switchport nonegotiate
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Vlan1
  no ip address
  shutdown
!
line con 0
!
line vty 0 4
  login
line vty 5 15
  login
!
!
end

```

从上面的输出中，找不到创建 VLAN 配置命令，交换机上的 VLAN 创建信息被保存在 `vlan.dat` 文件中，在 SW1 上使用 `dir` 命令查看交换机的 Flash 空间，显示如下：

```

SW1#dir
Directory of flash:/

   1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
   2  -rw-         676          <no date>  vlan.dat

32514048 bytes total (28098451 bytes free)

```

从上面的输出中，可以看到交换机的 Flash 中除了保存交换机的 IOS 文件外，还保存了 vlan.dat 文件，交换机的 VLAN 创建信息都保存在该文件中。

在 SW1 上使用“show vlan brief”命令，查看 SW1 的 VLAN 配置信息，显示如下：

```
SW1#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Gig1/1, Gig1/2
2 student	active	Fa0/1
3 teacher	active	Fa0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

从上面的输出中，可以看到 SW1 有两个新增的 VLAN，每个 VLAN 中还包含一个端口。Fa0/24 是主干端口，不属于任何一个 VLAN。使用 reload 命令重启 SW1，出现下面提示：

```
SW1#reload
```

```
Proceed with reload? [confirm] 提示是否确认要重新启动路由器，直接按回车键就是确认重启，按其他任意键取消重启。这里直接回车，重启交换机。
```

读者要知道在真实交换机上的提示与这里 Packet Tracer 模拟器中的有些不同，真实交换机上显示如下：

```
Switch#reload
```

```
System configuration has been modified. Save? [yes/no]:no
```

这里提示系统的配置发生了变化，是否要进行保存？Packet Tracer 模拟器中没有这样的提示。

```
Proceed with reload? [confirm] 按回车键重启，按任意键放弃重启。这里的提示与 Packet Tracer 相同。
```

SW1 重启完成后，使用“show run”命令查看交换机的配置，这里省去输出，读者可以发现交换机 SW1 的配置恢复到了默认配置。这是因为之前虽然配置了 SW1，但并没有保存。使用“show vlan brief”命令查看交换机上的 VLAN 信息，显示如下：

```
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
2 student	active	
3 teacher	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

上面的输出是不是有点出乎意料，虽然没有保存运行的配置文件，可之前创建的两个 VLAN 仍然存在，只是曾经划入两个 VLAN 的端口却不存在了。这是因为交换机的运行配置文件要保存才会存入 NVRAM 中，而交换机的 VLAN 信息自动保存在 Flash 的 vlan.dat

文件中，无须手工保存。至于两个 VLAN 中的端口为何又还原在默认的 VLAN 1 中，这是因为端口所属的 VLAN 配置信息保存在配置文件中，而不是 vlan.dat 中，有关这一点，读者在前面的“show run”命令中也可以证实。

可以通过删除 vlan.dat 文件，然后重启交换机来清除交换机上创建的所有 VLAN 信息。命令执行如下：

```
SW1#delete vlan.dat  
Delete filename [vlan.dat]?  
Delete flash:/vlan.dat? [confirm]
```

这里的 VLAN 信息不仅包括创建的 VLAN 号和名字，还包括 VTP（VLAN Trunking Protocol，VLAN 中继协议）的相关信息（有关 VTP，本书的下一章将会介绍）。如果有某些端口属于某一个 VLAN，然后删除了这个 VLAN，使用“show vlan”命令查看交换机 VLAN 信息的时候，将看不到这些端口，把这些所属 VLAN 被删除的端口称为游离端口，也就是无家可归的端口。读者可以添加被删除的 VLAN 或把这些游离端口划入其他存在的 VLAN 中，来让游离端口不再游离。

注意：在 Packet Tracer 中，如果一次没有完成一个实验，下次想继续完成这个实验，或者想把实验的结果保存起来，在交换机和路由器上使用“write”或“copy running-config startup-config”命令是无法办到的，但在真实的交换机或路由器上可以。在 Packet Tracer 中，保存配置使用的是“File”菜单中的“Save”子菜单命令，即使没有使用“write”或“copy running-config startup-config”命令保存交换机的配置文件，但一个“Save”子菜单命令可以保存当前所有网络设备的所有配置，相当于把当前的整个实验环境都保存在一个文件中。用户退出 Packet Tracer 时，会出现如图 10-3-9 所示的对话框，提示需不需要保存当前的实验环境。

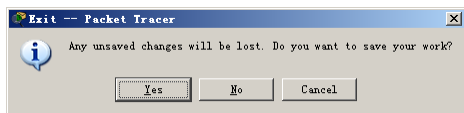


图 10-3-9 提示是否保存实验环境

如果文件已经存在，还会出现是否覆盖的提示。以后如果需要调出当前的实验环境，只要打开曾经保存的文件就可以了，这个功能真是非常方便。

10.3.6 用 Dynamips 模拟器配置 VLAN*

在 Packet Tracer 模拟器中配置 VLAN 和在 Dynamips 模拟器中配置 VLAN，配置的具体命令虽小有差异，但配置的思路是一样的：创建 VLAN，把端口加入 VLAN，配置主干链路，配置 VLAN 的一些可选信息（比如本地 VLAN 等），检验 VLAN 配置的正确性。

使用 Dynamips 模拟器，完成如图 10-3-10 所示的跨交换机的 VLAN 配置。

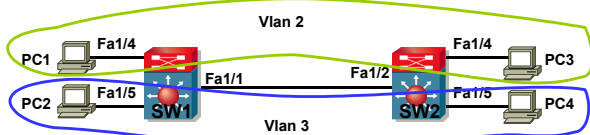


图 10-3-10 用 Dynamips 配置跨交换机的 VLAN

打开 CCNA 模拟器，启动 SW1、SW2、PC1、PC2、PC3、PC4 六台设备，完成如图 10-3-10 所示的 VLAN 配置。所有设备的配置如下，其中斜体部分为对配置的解释。

SW1 的配置如下：

```
Router#conf t
Router(config)#host SW1
SW1(config)#no cdp run  关闭 CDP 协议，不然会提示快速以太网双工不匹配。
SW1(config)#exit
SW1#vlan database  进入 VLAN 配置模式，Dynamips 只支持 VLAN 的数据库配置模式，不支持 VLAN 的全局配置模式。
SW1(vlan)#vlan 2 name student
SW1(vlan)#vlan 3 name teacher
SW1(vlan)#exit  添加的 VLAN 在 exit 或 apply 时才起作用，输入 abort 将放弃 VLAN 的修改。
SW1#conf t
SW1(config)#int fa 1/4
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 2
SW1(config-if)#int fa 1/5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 3
SW1(config-if)#int fa 1/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#int fa 1/2
SW1(config-if)#shutdown  关闭这个不使用的端口。
```

SW2 的配置如下：

```
Router#conf t
Router(config)#host SW2
SW2(config)#no cdp run
SW2(config)#exit
SW2#vlan database
SW2(vlan)#vlan 2 name student
SW2(vlan)#vlan 3 name teacher
SW2(vlan)#exit
SW2#conf t
SW2(config)#int fa 1/4
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 2
SW2(config-if)#int fa 1/5
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 3
SW2(config-if)#int fa 1/2
SW2(config-if)#switchport mode trunk
SW2(config-if)#int fa 1/1
SW2(config-if)#shutdown
```

PC1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host PC1
PC1(config)#no cdp run
PC1(config)#int fa 0/0
PC1(config-if)#ip add 192.168.1.1 255.255.255.0
PC1(config-if)#no shut
```

PC2、PC3、PC4 的配置与 PC1 的配置类似，只是 IP 地址不同，它们的 IP 地址分别是 192.168.1.2、192.168.1.3、192.168.1.4。在 PC1 上依次 ping PC2、PC3、PC4 的 IP 地址，测试网络的连通性，结果如图 10-3-11 所示，PC1 只能 ping 通 PC3，类似地，PC2 只能 ping 通 PC4。

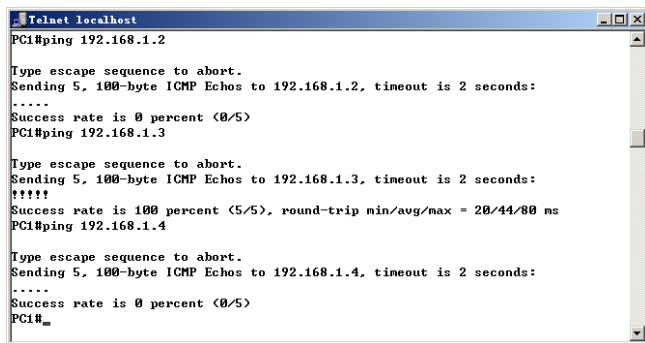


图 10-3-11 VLAN 测试结果

在 SW1 上验证 VLAN 的配置，因为 SW1 是在路由器上添加了交换模块来实现交换机的部分功能，并不是纯交换机，使用命令和纯交换机上使用的命令有细微的差异。执行“show vlan?”命令，显示如下：

```
SW1#show vlan?
vlan-range  vlan-switch  vlans
```

从上面的输出中，可以发现在路由交换机上，以“show vlan”开始的命令有三个。“show vlan-switch”命令用来查看 VLAN 的配置信息，相当于之前介绍过的“show vlan”命令。执行“show vlan-switch brief”命令，显示如下：

```
SW1#show vlan-switch brief
```

VLAN	Name	Status	Ports
1	default	active	Fa1/0, Fa1/2, Fa1/3, Fa1/6 Fa1/7, Fa1/8, Fa1/9, Fa1/10 Fa1/11, Fa1/12, Fa1/13, Fa1/14 Fa1/15
2	student	active	Fa1/4
3	teacher	active	Fa1/5
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

多次使用 Dynamips 模拟器，可能会在退出 VLAN 的数据库配置模式时，提示 Flash 空间不足，无法应用，退出失败，要求输入 abort，放弃 VLAN 的修改。显示如下：

```
SW1#vlan data
SW1(vlan)#vlan 3
VLAN 3 added:
  Name: VLAN0003
SW1(vlan)#exit
% not enough space on flash to store vlan database. trying squeeze...First creat
e squeeze log by erasing the entire device

% error squeezing flash - (Missing or corrupted log)
Error on database apply 40: NV storage failure
Use 'abort' command to exit
SW1(vlan)#abort
Aborting....
```

出现上述错误主要是因为模拟器的的问题。在交换机的特权模式下，执行“erase flash”命令，删除交换机的 Flash。系统会提示确认删除，在[confirm]后，直接按回车键确认删除，然后再次添加 VLAN，应用修改，可以成功退出。

```
SW1#erase flash
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Erase of flash: complete
SW1#vlan data
SW1(vlan)#vlan 3
VLAN 3 added:
    Name: VLAN0003
SW1(vlan)#exit
APPLY completed.
Exiting....
SW1#
```

这里介绍了在 **Dynamips** 模拟器中 **VLAN** 的配置。明白 **VLAN** 的配置原理后，不仅可以配置思科的交换机，还可以配置其他厂商的交换机，最多就是熟悉一下配置命令的差异。

10.4 VLAN 间路由***

实现 VLAN 间的互访可以借助于路由器或三层交换机。本节介绍几种实现 VLAN 间路由的方法。

10.4.1 基于路由器物理接口的 VLAN 间路由**

在图 10-4-1 中,SW1 交换机上配置了两个 VLAN,VLAN 1 的网络地址是 192.168.1.0/24,VLAN 2 的网络地址是 192.168.2.0/24。PC1 属于 VLAN 1,IP 地址是 192.168.1.1/24。PC2 属于 VLAN 2,IP 地址是 192.168.2.1/24。通过划分 VLAN,实现了 VLAN 1 和 VLAN 2 广播的隔离,提高了网络的安全。二层交换机无法提供不同 VLAN 之间的互访,需要借助三层以上(包括三层)的网络设备,比如路由器和三层交换机等。在图 10-4-1 中,路由器 R1 使用两个物理接口连接到交换机 SW1。R1 的 Fa0/0 连接到 SW1 的 Fa0/12,Fa0/12 属于 VLAN 1;R1 的 Fa0/1 连接到 SW1 的 Fa0/24,Fa0/24 属于 VLAN 2。路由器 R1 的 Fa0/0 接口的 IP 地址是 192.168.1.254/24,Fa0/1 接口的 IP 地址是 192.168.2.254/24。

读者可以在 Packet Tracer 模拟器中，搭建如图 10-4-2 所示的拓扑，或者直接打开光盘中的“配置\10\路由器实现 VLAN 间路由.pkt”文件。

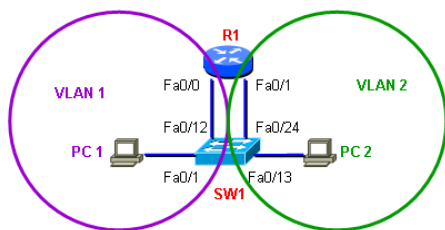


图 10-4-1 基于路由器物理接口的 VLAN 间路由示意图

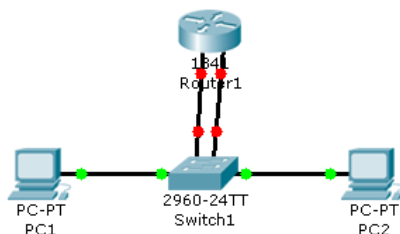


图 10-4-2 基于路由器物理接口的 VLAN 间路由拓扑图

(1) PC1 的配置

IP 地址: 192.168.1.1

掩码: 255.255.255.0

网关: 192.168.1.254

(2) PC2 的配置

IP 地址: 192.168.2.1

掩码: 255.255.255.0

网关: 192.168.2.254

(3) 交换机 SW1 的配置

```
Switch>en
Switch#conf t
Switch(config)#host SW1
SW1(config)#vlan 2
SW1(config-vlan)#int fa 0/1
SW1(config-vlan)#swi mode acc

SW1(config-if)#int fa 0/12
SW1(config-if)#swi mode acc
SW1(config-if)#int fa 0/13
SW1(config-if)#swi mode acc
SW1(config-if)#swi acc vlan 2
SW1(config-if)#int fa 0/24
SW1(config-if)#swi mode acc
SW1(config-if)#swi acc vlan 2
```

因为 VLAN 1 已经存在, 这里只需要创建 VLAN 2 就可以了。

连接 PC1 的交换机端口。

因为交换机上所有的端口默认都属于 VLAN 1, 这里只需要把端口配置成接入端口就可以了。

连接路由器 Fa0/0 接口的交换机端口。

连接 PC2 的交换机端口。

连接路由器 Fa0/1 接口的交换机端口。

(4) 路由器 R1 的配置

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.254 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int fa 0/1
R1(config-if)#ip add 192.168.2.254 255.255.255.0
R1(config-if)#no shut
```

(5) 测试

在 PC1 上 ping PC2 的 IP 地址 192.168.2.1, 结果显示可以 ping 通。通过使用路由器的不同物理接口连接到交换机上不同 VLAN 的端口, 并正确配置 IP 地址和网关, 可以实现不同 VLAN 之间的互相通信。

10.4.2 基于路由器子接口的 VLAN 间路由***

从上面的配置中可以看出, 如果使用路由器的物理接口来连接不同的 VLAN, 交换机上配置多少个 VLAN, 路由器上就需要有多少个物理接口, 此外还需要在交换机和路由器间连接多条线缆, 并占用交换机上的多个端口。现实中一般不使用这种互连方式, 使用路由器的不同物理接口互连交换机上多个 VLAN 的成本较高, 实现起来的难度也大。常见的做法是使用路由器的一个物理端口连接多个不同的 VLAN, 如图 10-4-3 所示, 有些文档上称之为“单臂路由”, 单臂路由是 CCNA 考试重点。

这里仍然使用如图 10-4-2 所示的拓扑图, 关闭 Packet Tracer 模拟器, 不要保存之前的实验配置。再次打开光盘中的“配置\10\路由器实现 VLAN 间路由.pkt”文件, PC1 和 PC2 的配置不变。

(1) SW1 的配置

```
Switch>en
Switch#conf t
Switch(config)#host SW1
```

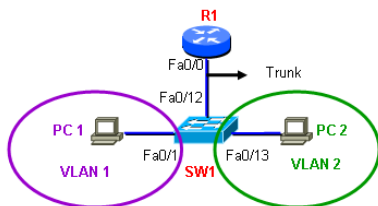


图 10-4-3 使用路由器子接口的 VLAN 间路由示意图

```
SW1(config)#vlan 2
SW1(config-vlan)#int fa 0/1      连接 PC1 的交换机端口。
SW1(config-vlan)#swi mode acc
SW1(config-if)#int fa 0/12
SW1(config-if)#swi mode trunk    把交换机连接路由器的端口配置成主干端口，在交换机和路
                                  由器间使用主干链路。
SW1(config-if)#int fa 0/13      连接 PC2 的交换机端口。
SW1(config-if)#swi mode acc
SW1(config-if)#swi acc vlan 2
```

(2) R1 的配置

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0            路由器只使用一个物理接口，来互连交换机上的多个 VLAN。物理接
                                  口只需要打开，不需要额外的配置。

R1(config-if)#no shut
R1(config-if)#exit
R1(config)#int fa 0/0.?
使用 CLI 在线帮助，查看路由器子接口的编号。路由器只使用一个物理接口，来互连交换机上的多个 VLAN，
每个 VLAN 的网关都指向路由器。路由器虽然只有一个物理接口，但可以启用子接口，可以把每个子接口想象
成一个物理接口。从下面的输出中可以看出路由器的一个物理接口可以支持几十亿个子接口。
<0-4294967295> FastEthernet interface number
R1(config)#int fa 0/0.1
使用第一个子接口作为 VLAN 1 的网关。子接口编号和 VLAN 号之间没有必然的关系，这里使用的是子接口 1，
也可以使用子接口 100。为了便于查看，一般习惯上喜欢把子接口号和 VLAN 号设成相同的数字。子接口默认
是打开状态，不需要使用“no shutdown”命令进行打开。
R1(config-subif)#encapsulation dot1Q 1
配置子接口的封装协议是 dot1Q，也就是 802.1Q，这里使用的封装协议要与交换机主干端口的封装协议相同。
思科有些型号的交换机可以支持 dot1Q 和 ISL 的封装协议，有些型号的交换机只能支持 dot1Q 封装协议。尤
其是现在新出厂的交换机，默认的封装协议就是 dot1Q。这里的“1”指的是 VLAN 的编号，这里的 1 不能随便
输入，要与交换机上的 VLAN 号对应起来。
R1(config-subif)#ip address 192.168.1.254 255.255.255.0    路由器子接口的 IP 地址，这
                                                              里配置的是 VLAN 1 的网关。
R1(config-subif)#int fa 0/0.200    配置 Fa0/0 物理接口的第 200 个子接口，子接口并不具有
                                    实际的意义，仅仅是一个接口的编号。
R1(config-subif)#enca dot 2    子接口 200 被封装的协议是 dot1Q，相关的 VLAN 号是 2。
R1(config-subif)#ip add 192.168.2.254 255.255.255.0    路由器子接口的 IP 地址，这里配置
                                                          的是 VLAN 2 的网关。
```

给子接口配置 IP 地址前，一定要先封装协议，顺序不要颠倒。如果给一个没有封装协议的子接口配置 IP 地址，将会收到下面的错误提示信息：

```
% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.
```

这里是报错信息，IP 地址配置命令失败。提示局域网子接口只有被封装 802.10、802.1Q 或 ISL 协议后，才可以被配置 IP 地址。

(3) 测试

在 PC1 上 ping PC2 的 IP 地址 192.168.2.1，结果显示可以 ping 通。通过配置路由器和交换机间的主干链路，使用路由器子接口实现不同 VLAN 之间的互相通信。

不要关闭该实验，继续下面的学习。

10.4.3 交换机上的端口类型*

思科交换机的端口类型有三种：交换端口（switchport）、路由端口（no switchport）和 SVI 端口（Switch Virtual Interface，交换机虚拟端口）。交换端口是一个二层端口，不能配

置三层的 IP 地址；路由端口和 SVI 端口都是三层端口，可以配置 IP 地址。

1. 二层交换机

思科二层交换机（比如 2900 系列、3500、3550-SMI 交换机等）只有两种类型的端口：交换端口和 SVI 端口。

交换端口：二层交换机上的物理端口就是一个二层的交换端口。

SVI 端口：二层交换机也可以被配置一个 IP 地址，来实现对交换机的远程管理。通过下面的配置命令，给 SW1 交换机配置一个网管的 IP 地址。

```
SW1(config)#int vlan 1
SW1(config-if)#ip add 192.168.1.100 255.255.255.0
SW1(config-if)#no shut
```

对三层的 SVI 端口，要使用 “no shutdown” 命令。

配置完成后，在 PC1 上测试到 192.168.1.100 的连通性，结果可以成功 ping 通。在 PC2 上测试到 192.168.1.100 的连通性，结果 ping 失败。交换机 SW1 被配置 IP 地址，但没有配置网关，不能和非同一子网的设备进行通信。可以使用下面的命令，给 SW1 配置默认网关：

```
SW1(config)#ip default-gateway 192.168.1.254
```

配置完成后，再次在 PC2 上测试到 192.168.1.100 的连通性，结果可以成功 ping 通。192.168.1.100 是 SW1 的网管 IP 地址，是不是交换机的网管 IP 地址一定要配置在 VLAN 1 上呢？不是的，看下面的配置：

```
SW1(config)#int vlan 2
SW1(config-if)#ip add 192.168.2.100 255.255.255.0
SW1(config-if)#no shut
```

配置 SW1 的 SVI2 端口。
使用 “no shutdown” 命令激活端口。

读者猜测一下，PC1 和 PC2 到 SW1 的连通性是什么样的？结果是 PC1 只可以 ping 通 192.168.1.100，PC2 可以 ping 通 192.168.1.100 和 192.168.2.100，这是因为交换机的默认网关与 VLAN 1 在同一个子网中，VLAN 1 的 IP 地址支持跨网访问，VLAN 2 的 IP 地址不支持跨网访问。在 SW1 上使用 “show ip int brief” 命令，查看 SW1 上 IP 地址的配置情况，显示如下：

```
SW1#show ip int brief
Interface      IP-Address      OK? Method Status  Protocol
FastEthernet0/1 unassigned      YES manual up      up
省略部分输出。
Vlan1          192.168.1.100   YES manual up      up
Vlan2          192.168.2.100   YES manual up      up
```

从上面的输出中，可以看到 SW1 的 VLAN 1 和 VLAN 2 都被配置了 IP 地址，并且显示状态是正常的。在思科部分老款的交换机上，VLAN 2 状态会显示为 “manual administratively down”，也就是说，在已有较小 SVI 端口有效的情况下，较大 SVI 端口的 no shut 命令并不起作用。

2. 三层交换机

！ 注意：CCNA 考试中不涉及三层交换机的内容，本节接下来的内容均与 CCNA 考试无关。如果你不想成为一个 Paper（纸质）CCNA，请完成本节的所有实验。CCNA 考试中虽不涉及三层交换机，但三层交换机却在工程中被大量使用，几乎所有企业的核心都配备了三层交换机。

思科三层交换机（比如 3550-EMI、3560、3750，以及更高档的交换机）有三种类型的

端口：交换端口、路由端口和 SVI 端口。Dynamips 模拟器机架中的 SW1、SW2 和 SW3 都是路由交换机，相当于三层交换机。

三层交换机上也支持二层的交换端口和三层的 SVI 端口。此外，三层交换机还支持路由端口。运行 Dynamips 模拟器机架中的 SW1：

```
Router>en
Router#conf t
Router(config)#host SW1
SW1(config)#int fa 1/6
SW1(config-if)#ip add 1.1.1.1 255.255.255.0

% IP addresses may not be configured on L2 links.
试图给一个二层的交换机端口配置 IP 地址。路由器提示，命令错误，IP 地址不能被配置在一个二层的链路上。
SW1(config-if)#no switchport
在三层交换机上使用“no switchport”命令，取消一个端口的交换端口特性，该端口就成了一个三层的端口，也称为路由端口。该三层交换机上的路由端口虽具有了路由端口的特性，比如可以配置 IP 地址等，但也失去了二层交换端口的特性，比如不可以配置端口安全等。可以在端口下使用 switchport 命令把端口从路由端口改回到二层交换端口。
SW1(config-if)#ip add 1.1.1.1 255.255.255.0
SW1(config-if)#
```

Packet Tracer 模拟器中也提供了一款三层交换机，型号是 3560。

10.4.4 基于三层交换机的 VLAN 间路由

为了大家可以更好地区分二层交换机和三层交换机，这里先使用 Dynamips 模拟机架中完成 10.4.2 节类似的单臂路由实验，然后关闭路由器，使用三层交换机来提供 VLAN 间的路由，最后给出在 Packet Tracer 模拟器中三层交换机的配置。

1. 单臂路由

打开 Dynamips 模拟器的 CCNA 机架，运行 SW1、R1、PC1、PC2 这 4 台设备，这里把 SW1 想象成一台二层的 VLAN 型交换机（三层交换机没有额外配置的情况下，可以当成二层交换机使用），R1 是一台路由器。每个设备的 IP 地址配置如图 10-4-4 所示。

R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#no cdp run
R1(config)#int fa 2/0
R1(config-if)#no shut 打开物理接口
R1(config-if)#int fa 2/0.1
R1(config-subif)#encapsulation dot1Q 1
R1(config-subif)#ip add 192.168.1.254 255.255.255.0
R1(config-subif)#int fa 2/0.2
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#ip add 192.168.2.254 255.255.255.0
```

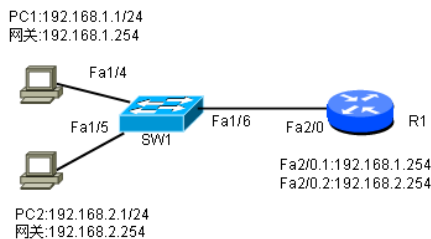


图 10-4-4 单臂路由

SW1 的配置如下:

```
Router#conf t
Router(config)#host SW1
SW1(config)#no cdp run
SW1(config)#no ip routing 关闭三层交换机的路由功能, 让它模拟二层交换机, 不关闭也没有关系,
                           因为本实验中并没有配置三层。
SW1(config)#exit
SW1#vlan database
SW1(vlan)#vlan 2
SW1(vlan)#exit
SW1#conf t
SW1(config-if)#int fa 1/5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 2
SW1(config-if)#int fa 1/6
SW1(config-if)#switchport mode trunk
```

PC1 的配置如下:

```
Router>en
Router#conf t
Router(config)#host PC1
PC1(config)#no cdp run
PC1(config)#int fa 0/0
PC1(config-if)#ip add 192.168.1.1 255.255.255.0
PC1(config-if)#no shut
PC1(config-if)#exit
PC1(config-if)#no ip routing 关闭路由器的路由功能, 让它模拟一台计算机。
PC1(config)#ip default-gateway 192.168.1.254
配置计算机的网关, 对于关闭路由协议的路由设备, 要使用这条命令来指定默认路由; 如果没有关闭路由协议,
使用 ip route 0.0.0.0 0.0.0.0 配置默认路由。
```

PC2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host PC2
PC2(config)#no cdp run
PC2(config)#int fa 0/0
PC2(config-if)#ip add 192.168.2.1 255.255.255.0
PC2(config-if)#no shut
PC2(config-if)#exit
PC2(config-if)#no ip routing
PC2(config)#ip default-gateway 192.168.2.254
```

在 PC1 上 ping 192.168.2.1, 发现可以 ping 通 PC2。关闭路由器 R1 的 Fa2/0 端口后, 再次在 PC1 上 ping 192.168.2.1, 发现 ping 不通了, 原因是 PC1 和 PC2 分属于不同的网段, 没有一个三层设备来提供路由, 它们之间无法进行通信。不要关闭该机架, 继续后面的实验。

2. 三层交换机的 VLAN 间路由

为了节省时间, 在单臂路由配置的基础上, 做些改动来完成三层交换。关闭 4 台设备中的 R1, 开启 SW1 的路由功能, PC1 和 PC2 的配置保持不变。每个设备的 IP 地址配置如图 10-4-5 所示。

SW1 的配置如下:

```
SW1(config)#ip routing 开启三层交换机的路由功能, 为不同子网间的数据包提供路由转发功能。
SW1(config)#int vlan 1 配置三层交换机的 SVI 端口, 这里的 SVI 端口相当于路由器的一个端口, 只不过这是一个虚拟的端口, 是一个看不见的端口。
SW1(config-if)#ip add 192.168.1.254 255.255.255.0
SW1(config-if)#no shut
SW1(config-if)#int vlan 2
在三层交换机上, 可以配置多个 SVI 端口, 多个 SVI 端口的 IP 地址可以同时有效。而二层交换机上只能有一
```

个 IP 地址有效。

```
SW1(config-if)#ip add 192.168.2.254 255.255.255.0
SW1(config-if)#no shut
```

PC1 和 PC2 的配置同单臂路由实验中的配置，在 PC1 上 ping PC2 的地址 192.168.2.1，发现可以 ping 通，如果是在单臂路由实验的基础上配置本实验，可能会 ping 不通。因为 PC1 和 PC2 上已经缓存了它们网关的 MAC 地址，那个 MAC 地址还是 R1 的 Fa2/0 的 MAC 地址，可以使用“show arp”命令查看，使用“clear arp”命令清除 ARP 缓存，然后再 ping 测试，配置无误就可以 ping 通了。

```
PC1#show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.1.1 - cc03.0530.0000 ARPA FastEthernet0/0
Internet 192.168.1.254 9 cc00.0530.0000 ARPA FastEthernet0/0
PC1#clear arp
```

读者还要注意代理 ARP 的问题，在代理 ARP 启用的情况下，即使 PC 不配置网关，也可以跨网段通信。可以在端口下使用“no ip proxy-arp”命令关闭代理 ARP 功能。

3. Packet Tracer 中的配置

在 Packet Tracer 模拟器中，完成图 10-4-6 中的配置，其中思科 3560 交换机的配置如下：

```
Switch>en
Switch#conf t
Switch(config)#vlan 2
Switch(config-vlan)#int fa 0/5
Switch(config-if)#swi mode acc
Switch(config-if)#swi acc vlan 2
Switch(config-if)#int vlan 1
Switch(config-if)#ip add 192.168.1.254 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#int vlan 2
Switch(config-if)#ip add 192.168.2.254 255.255.255.0
Switch(config-if)#no shut
```

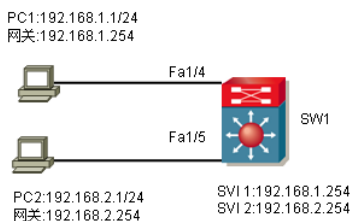


图 10-4-5 三层交换

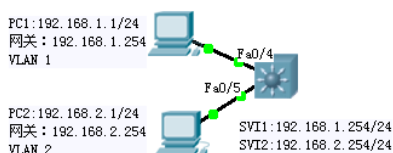


图 10-4-6 Packet Tracer 中的三层交换

10.4.5 路由器和三层交换机在实现 VLAN 间路由上的差异

从前面的实验中，可以发现路由器可以互连不同的 VLAN，三层交换机也可以互连不同的 VLAN。两种互连 VLAN 的方式有什么区别呢？

在图 10-4-7 中，左边是前面介绍过的基于路由器物理接口的 VLAN 间路由。不管是基于物理接口还是基于子接口的 VLAN 间路由，不同 VLAN 间的通信都要流经路由器。现在分析一下使用路由器实现 VLAN 间路由的劣势：首先是速度问题，前面介绍过数据包流经路由器的延时比流经交换机的延时要大，因为路由器比交换机的处理过程要复杂，解封装—查询路由表—再封装；其次是带宽瓶颈问题，在图 10-4-7 的左图中，VLAN 1 去往 VLAN 2 的数据包都要流经路由器，如果两个 VLAN 中有多台主机同时通信，交换机和路由器之

间的链路将成为瓶颈。每台计算机都可以 100Mb/s 到交换机，可多台 VLAN 1 中的计算机只能共享 100Mb/s 链路到 VLAN 2 中的计算机。

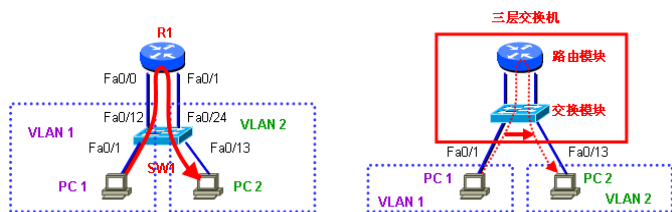


图 10-4-7 三层交换

在图 10-4-7 中，右边是前面介绍过的使用三层交换机的 VLAN 间路由。假设 VLAN 1 中的 PC1 要访问 VLAN 2 中的 PC2，PC1 把数据包发给三层交换机上的 SVI 端口，三层交换机知道这是 VLAN 间的通信，三层交换机把数据包发往三层交换机上的路由模块，可以形象地把这里的路由模块想象成路由器。路由模块解封封装数据包，查询到 PC2 的 MAC 地址，然后进行封装，封装后的数据包被转发给三层交换机上的交换模块，交换模块查询 MAC 地址表，把数据帧从交换机的 Fa0/13 端口发出。是不是感觉三层交换机和路由器的处理没什么区别，其实不然，前面只是 PC1 发往 PC2 第一个数据包的处理过程，当 PC1 继续有数据包发往 PC2 时，三层交换机查询缓存，不用把数据包转发给路由模块，直接修改数据帧头中的源和目的 MAC 地址后，把数据帧从 Fa0/13 端口发出。三层交换机对不同 VLAN 间数据包的处理过程是“一次路由，多次交换”，即第一个数据包需要路由，后续的数据包直接交换，这样数据包的转发延迟被大大降低。VLAN 1 发往 VLAN 2 的数据包被交换机的背板转发，交换机的背板带宽远远超过端口的链路带宽，比如思科 3560G-24TS 交换机的背板带宽是 32Gb/s，这样不同 VLAN 间数据包的转发不存在链路带宽的瓶颈问题。

经过上述比较，相信读者可以明白为何现在多数企业的核心都是使用三层或多层交换机来实现部门之间的路由，而不是使用路由器来实现部门之间的路由。



10.5 VLAN 故障排除**

VLAN 故障包括：端口错、IP 错、网关错、本地 VLAN 不匹配、Trunk 模式不匹配、Trunk 允许的 VLAN 不匹配。

本节结合实验，介绍 VLAN 故障排除的方法。某公司拓扑如图 10-5-1 所示，PC1 和 PC2 属于 VLAN 2，PC3 属于 VLAN 3。VLAN 2 的 IP 子网是 192.168.2.0/24，VLAN 3 的 IP 子网是 192.168.3.0/24。PC1 的 IP 地址是 192.168.2.1/24，PC2 的 IP 地址是 192.168.2.2/24，PC3 的 IP 地址是 192.168.3.1/24。SW1 和 SW2 都是二层交换机，路由器 R1 使用子接口实现 VLAN 间路由。经测试，发现 PC1 ping 不通 PC2 和 PC3，请找出问题所在，并改正错误，使 PC1 可以成功 ping 通 PC2 和 PC3。

PC、交换机和路由器的配置都已完成，读者在 Packet Tracer 模拟器中打开光盘中的“配置\10\vlan 故障排除.pkt”，大约一分钟后，Packet Tracer 模拟器中的拓扑显示如图 10-5-2 所示。通过 CCNA 考试，并不代表真正具备了 CCNA 的能力，因为有很多工程经验还要在实践中不断积累。这里给大家提供了一个锻炼的机会，读者先自行排错，然后再继续阅读后面的内容。

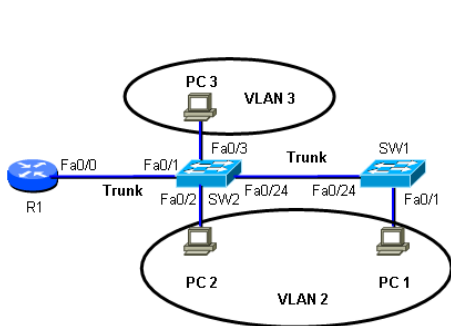


图 10-5-1 某公司拓扑示意图

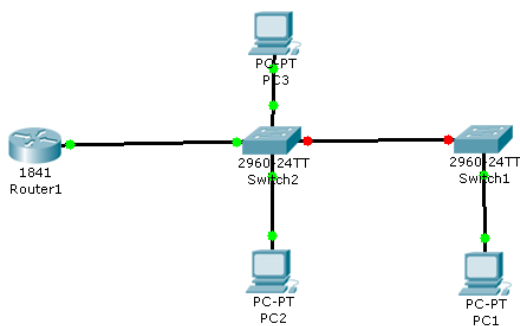


图 10-5-2 Packet Tracer 中拓扑

1. 物理层排错

从图 10-5-2 中可以看出 SW1 和 SW2 之间使用的是直通型双绞线，同种设备间应该使用交叉线才对，但因拓扑中使用的是思科 2960 交换机，这种型号的交换机端口可以自适应线缆类型，不管是直通还是交叉线都没有问题。如果发现 SW1 和 SW2 之间链路的颜色是红色，表明链路不正常，首先检查物理层是否正常。在二层交换机上，端口默认都是打开的，如果不放心可以使用“show ip int brief”命令检查链路是否被关闭，既然端口是打开的，链路却不正常，很可能是线缆有问题，更换成正确的线缆。

检测线缆两端设备的接口是否正确。现实中可以理理线，Packet Tracer 模拟器中只要把鼠标停留在链路上，即可显示链路两端所连设备的端口，或者单击菜单“选项”→“首选项”，选中“显示端口标签”。从中发现 PC2 连接到 SW2 的 Fa0/3 端口，PC3 连接到 SW2 的 Fa0/2 端口，两台 PC 的连接端口与图 10-5-1 中不同，删除 SW2 与 PC2 和 PC3 之间的线缆，重新连接正确的端口。

2. 数据链路层排错

数据链路层的问题有封装协议是否正确，时钟是否设置等。涉及跨交换机的配置，还要分析主干链路的配置是否正确，这里把与 VLAN 相关的验证都放到网络层讨论。

因为这里都是以太网，没有同步串行链路，不需要考虑时钟问题。这里配置的是单臂路由，涉及路由器子接口的封装，在路由器 R1 上使用“show run”命令查看子接口的封装，关键部分显示如下：

```
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.2
encapsulation dot1Q 200
ip address 192.168.2.254 255.255.255.0
!
interface FastEthernet0/0.3
encapsulation dot1Q 3
ip address 192.168.3.254 255.255.255.0
```

从上面的输出中，可以看到路由器子接口的封装协议是 dot1Q，与交换机上的相同，但 FastEthernet0/0.2 子接口封装的是 dot1Q 200，这里的 200 是指 VLAN 号，配置错误，正确的 VLAN 号应该是 2。这里之所以配错，原因很可能是用户没有分清子接口和 VLAN 号的关系，错误地认为子接口编号就是 VLAN 号。事实上，子接口编号与 VLAN 编号之间没有

任何关系，与 VLAN 编号有关系的是子接口封装的 VLAN 标识。

使用下面的命令封装路由器 FastEthernet0/0.2 子接口：

```
R1(config)#int fa 0/0.2
R1(config-subif)#encapsulation dot1q 2
```

3. 网络层排错

网络层的排错难度很大，涉及 IP 地址配置、VLAN 创建、端口分配、Trunk 模式、Trunk 链路上允许的 VLAN、Trunk 链路的本地 VLAN。

(1) IP 地址排错

检查 PC1、PC2、PC3 的 IP 地址，子网掩码和网关的配置是否正确。PC1 和 PC2 的配置均正确，PC3 的网关被错误地配置成 192.168.3.2 了，把它改成 192.168.3.254，即路由器 R1 FastEthernet0/0.3 子接口的 IP 地址。

(2) 本地 VLAN 排错

SW1 上不停出现 “%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/24 (2), with SW2 FastEthernet0/24 (1).” 报错信息，提示本地主干端口 FastEthernet0/24 的本地 VLAN 是 2，而 SW2 主干端口 FastEthernet0/24 的本地 VLAN 是 1，两端主干端口的本地 VLAN 不一致，使用下面的命令把 SW1 端口 FastEthernet0/24 的本地 VLAN 改成 1。

```
SW1(config)#int fa 0/24
SW1(config-if)#swi trunk native vlan 1
```

(3) 主干链路排错

查看 SW1 上的主干端口是否正确，显示如下：

```
SW1#show int fa 0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

从上面的输出中，可以看出 SW1 的 Fa0/24 端口配置的模式是 Trunk，端口的状态是 Trunk，DTP 协议被关闭，主干上允许传输所有的 VLAN。

查看 SW2 上的主干端口是否正确，显示如下：

```
SW2#show int fa 0/24 switchport
Name: Fa0/24
Switchport: Enabled
```

```

Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none

```

从上面的输出中，可以看出 SW2 的 Fa0/24 端口配置的模式是 Dynamic desirable，端口的状态是 static access，DTP 协议被打开，主干上允许传输所有的 VLAN。

在 SW2 上使用 “show interface trunk” 命令查看工作在主干模式，显示如下：

```

SW2#show int trunk
Port      Mode      Encapsulation Status      Native vlan
Fa0/1     on        802.1q      trunking     1

Port      Vlans allowed on trunk
Fa0/1     2

Port      Vlans allowed and active in management domain
Fa0/1     ,2

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     ,2

```

从上面的输出中，可以看到主干端口只有 Fa0/1，Fa0/24 并没有工作在主干模式。

至于为何不能协商成主干链路，10.2.4 节有介绍。一边是 Trunk，一边是 Access，主干链路失败。修改 SW2 的 Fa0/24 端口的主干模式，命令如下：

```

SW2(config)#int fa 0/24
SW2(config-if)#swi mode trunk
SW2(config-if)#switchport nonegotiate

```

此时，测试 PC1 可以正常 ping 通 PC2，但 PC2 无法 ping 通 PC3。继续后面的排错。

(4) VLAN 创建和端口分配排错

查看 SW1 上 VLAN 划分是否正确，显示如下：

```

SW1#show vlan brief

```

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Gig1/1, Gig1/2
2 VLAN0002	active	Fa0/1
3 VLAN0003	active	
1002 fddi-default	active	
1003 token-ring-default	active	


```
1004 fddinet-default    active
1005 trnet-default      active
```

从上面的输出中，可以看出 SW1 上的 VLAN 创建和端口分配正确。

查看 SW2 上 VLAN 划分是否正确，显示如下：

```
SW2#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig1/1, Gig1/2
2	VLAN0002	active	Fa0/2, Fa0/3
3	VLAN0003	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

从上面的输出中，可以看出 SW2 上的 VLAN 创建正确，但端口分配不正确，把 Fa0/3 错误地分配到 VLAN 2 中，该端口连接 PC3，应该被分配到 VLAN 3 中。使用下面的命令更正这个错误。

```
SW2(config)#int fa 0/3
SW2(config-if)#swi acc vlan 3
```

继续测试 PC1 到 PC3 的通信，结果 ping 仍然失败。

(5) 主干链路允许的 VLAN 排错

查看 SW2 的主干端口，显示如下：

```
SW2#show int fa 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

Packet Tracer 模拟器毕竟是模拟器，这里的输出有误，不应该显示允许所有的 VLAN，而应该显示成“Trunking VLANs Enabled: 2”。换一个命令，查看 SW2 上有哪些主干端口，显示如下：

```
SW2#show int trunk
Port      Mode      Encapsulation  Status  Native vlan
```

```

Fa0/1    on      802.1q    trunking    1
Fa0/24   on      802.1q    trunking    1

Port      Vlans allowed on trunk
Fa0/1     2
Fa0/24    1-1005

Port      Vlans allowed and active in management domain
Fa0/1     ,2
Fa0/24    1,2,1002,1003,1004,1005

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     ,2
Fa0/24    1,2,1002,1003,1004,1005

```

从上面的输出中，可以看出 Fa0/1 主干端口仅允许传输 VLAN 2 的信息。PC1 和 PC3 通信，数据包需要流经路由器 R1，而 SW2 的 Fa0/1 端口仅允许 VLAN 2 的流量，不允许 VLAN 3 的流量，也就是不允许 PC3 的流量传输，PC1 当然无法 ping 通 PC3。

使用下面的命令取消 SW2 Fa0/1 端口的 VLAN 限制，允许传输所有的 VLAN。

```

SW2(config)#int fa 0/1
SW2(config-if)#no switchport trunk allowed vlan

```

继续测试 PC1 到 PC3 的通信，此时可以 ping 通。

至此，故障排除结束。

工程经验：读者分别在 Dynamips 和 Packet Tracer 完成图 10-5-3 中的实验配置，使 PC1 和 PC3 可以相互访问。多数读者在 Packet Tracer 模拟器中可以完成这一实验，在 Dynamips 模拟器中却完不成。结论就是 Packet Tracer 模拟器的 Bug 导致这一实验容易完成，在 Dynamips 和真实交换机中又容易忽视的一点，将导致网络连通失败。有关这部分内容的详细讲解和演示，请参考光盘中的视频文件“10-2.wrf”。

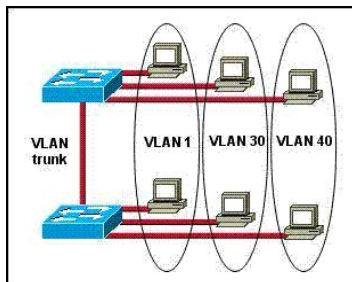


图 10-5-3 VLAN 跨多台交换机的传输



10.6 真题精选***

1. Refer to the exhibit. How many broadcast domains exist in the exhibited topology?



- A. one
- D. four

- B. two
- E. five

- C. three
- F. six

2. Which two statements describe the Cisco implementation of VLANs? (Choose two.)

- A. VLAN 1 is the default Ethernet VLAN.
- B. CDP advertisements are only sent on VLAN 1002.
- C. By default, the switch IP address is in VLAN 1005.
- D. VLANs 1002 through 1005 are automatically created and cannot be deleted.

3. Refer to the exhibit. A network administrator is unable to connect remotely to a device and initiates a console session. The administrator executes the show ip interface brief command. Why did the remote connection fail?

```
ORL# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	manual	up	up
FastEthernet0/2	unassigned	YES	manual	up	up
<output omitted>					
GigabitEthernet1/1	unassigned	YES	manual	down	down
GigabitEthernet1/2	unassigned	YES	manual	down	down
Vlan1	192.168.1.100	YES	manual	administratively down	down

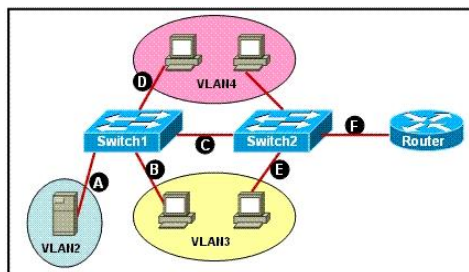
- A. The Gigabit Ethernet interfaces are not up
- B. VLAN 1 is shut down.
- C. The switch needs to have a clock rate entered on one of its interfaces.
- D. The switch does not have a management IP address assigned.

4. Refer to the exhibit. Which two statements about the configuration of the switch interface are correct? (Choose two.)

```
SwitchA(config)# interface fa0/0
SwitchA(config-if)# switchport access vlan 2
```

- A. The switchport belongs only to VLAN 2
- B. Interface fa0/0 will be in both VLAN 1 (by default) and VLAN 2
- C. The exhibit shows interface fa0/0 to be dynamically mapped to VLAN 2
- D. A network host can be connected to this interface.

5. Refer to the exhibit. A network associate needs to configure the switches and router in the graphic so that the hosts in VLAN3 and VLAN4 can communicate with the enterprise server in VLAN2. Which two Ethernet segments would need to be configured as trunk links? (Choose two.)



- | | | |
|------|------|------|
| A. A | B. B | C. C |
| D. D | E. E | F. F |

6. When a new trunk is configured on a 2950 switch, which VLANs by default are allowed over the trunk link?

- A. no VLANs
- B. all VLANs
- C. only VLANs 1 - 64
- D. only the VLANs that are specified when creating the trunk

7. When a new trunk link is configured on an IOS based switch, which VLANs are allowed over the link?

- A. By default, all defined VLANs are allowed on the trunk.
- B. Each single VLAN, or VLAN range, must be specified with the switchport mode command.
- C. Each single VLAN, or VLAN range, must be specified with the vtp domain command.
- D. Each single VLAN, or VLAN range, must be specified with the vlan database command.

8. Which are valid modes for a switch port used as a VLAN trunk? (Choose three.)

- | | | |
|----------------|-------------|---------------|
| A. transparent | B. auto | C. on |
| D. desirable | E. blocking | F. forwarding |

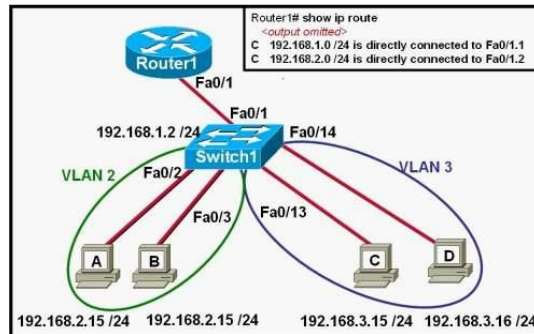
9. What is the function of the command switchport trunk native vlan 999 on a Cisco Catalyst switch?

- A. It creates a VLAN 999 interface.
- B. It designates VLAN 999 for untagged traffic.
- C. It blocks VLAN 999 traffic from passing on the trunk.
- D. It designates VLAN 999 as the default for all unknown tagged traffic.

10. A company is installing IP phones. The phones and office computers connect to the same device. To ensure maximum throughput for the phone data, the company needs to make sure that the phone traffic is on a different network from that of the office computer data traffic. What is the best network device to which to directly connect the phones and computers, and what technology should be implemented on this device? (Choose two.)

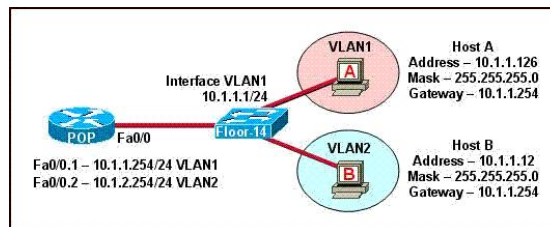
- | | | |
|--------|------------------|-----------|
| A. hub | B. router | C. switch |
| D. STP | E. subinterfaces | F. VLAN |

11. Refer to the exhibit. The network administrator has created a new VLAN on Switch1 and added host C and host D. The administrator has properly configured switch interfaces FastEthernet0/13 through FastEthernet0/24 to be members of the new VLAN. However, after the network administrator completed the configuration, host A could communicate with host B, but host A could not communicate with host C or host D. Which commands are required to resolve this problem?



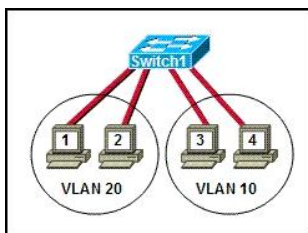
- A. Router(config)# interface fastethernet 0/1.3
 Router(config-if)# encapsulation dot1q 3
 Router(config-if)# ip address 192.168.3.1 255.255.255.0
- B. Router(config)# router rip
 Router(config-router)# network 192.168.1.0
 Router(config-router)# network 192.168.2.0
 Router(config-router)# network 192.168.3.0
- C. Switch1# vlan database
 Switch1(vlan)# vtp v2-mode
 Switch1(vlan)# vtp domain cisco
 Switch1(vlan)# vtp server
- D. Switch1(config)# interface fastethernet 0/1
 Switch1(config-if)# switchport mode trunk
 Switch1(config-if)# switchport trunk encapsulation isl

12. The network shown in the diagram is experiencing connectivity problems. Which of the following will correct the problems? (Choose two.)



- A. Configure the gateway on Host A as 10.1.1.1.
- B. Configure the gateway on Host B as 10.1.2.254.
- C. Configure the IP address of Host A as 10.1.2.2.
- D. Configure the IP address of Host B as 10.1.2.2.
- E. Configure the masks on both hosts to be 255.255.255.224.
- F. Configure the masks on both hosts to be 255.255.255.240.

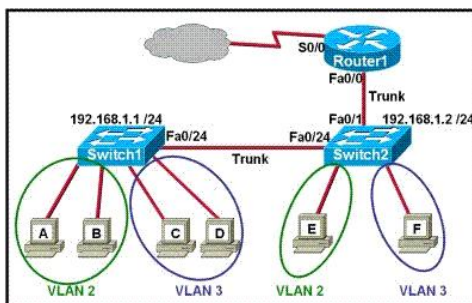
13. Refer to the exhibit. Hosts on the same VLAN can communicate with each other but are unable to communicate with hosts on different VLANs. What is needed to allow communication between VLANs?



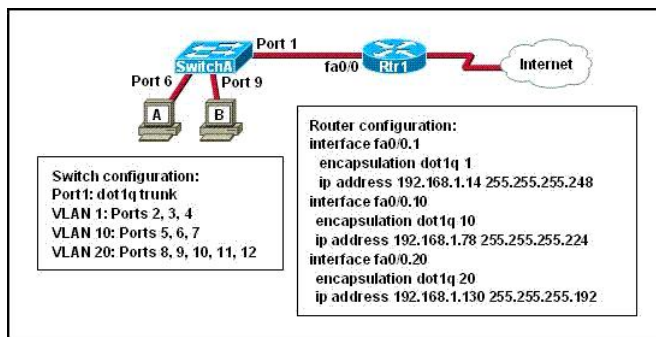
- A. a switch with a trunk link that is configured between the switches
- B. a router with an IP address on the physical interface that is connected to the switch
- C. a switch with an access link that is configured between the switches
- D. a router with subinterfaces configured on the physical interface that is connected to the switch

14. Refer to the exhibit. Which two statements are true about interVLAN routing in the topology that is shown in the exhibit? (Choose two.)

- A. Host E and host F use the same IP gateway address.
- B. Router1 and Switch2 should be connected via a crossover cable.
- C. Router1 will not play a role in communications between host A and host D.
- D. The FastEthernet 0/0 interface on Router1 must be configured with subinterfaces.
- E. Router1 needs more LAN interfaces to accommodate the VLANs that are shown in the exhibit.
- F. The FastEthernet 0/0 interface on Router1 and Switch2 trunk ports must be configured using the same encapsulation type.



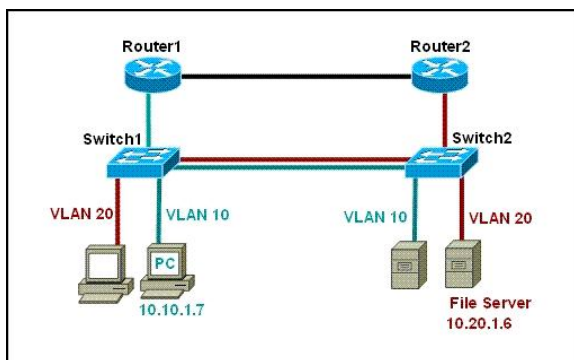
15. Refer to the exhibit. A network administrator is adding two new hosts to SwitchA. Which three values could be used for the configuration of these hosts? (Choose three.)



- A. host 1 IP address: 192.168.1.79
- B. host 1 IP address: 192.168.1.64
- C. host 1 default gateway: 192.168.1.78
- D. host 2 IP address: 192.168.1.128
- E. host 2 default gateway: 192.168.1.129
- F. host 2 IP address: 192.168.1.190

16. Refer to the exhibit. The network manager is evaluating the efficiency of the current network design. RIPv2 is enabled on all Layer 3 devices in the network. What network devices participate in passing traffic from the PC at 10.10.1.7 to File Server at 10.20.1.6 in the order that they will forward traffic from source to destination?

- A. Switch1, Switch2
- B. Switch1, Switch2, Router2, Switch2
- C. Switch 1, Router1, Switch1, Switch2
- D. Switch1, Router1, Router2, Switch2



10.7 真题解答***

1. 解：C

题目问：参照图，图中的拓扑存在几个广播域？关于广播域的问题，在默认的情况下，每个交换机是不能隔离广播域的，所以在同一个区域的所有交换机都在同一个广播域中。但是为了减少广播的危害，将广播限制在一个更小的范围，有了 VLAN 的概念，VLAN 表示的是一个虚拟的局域网，可以隔离广播。被 VLAN 隔离的每个区域都表示一个单独的广播域，这样一个 VLAN 中的广播流量不能传到其他 VLAN 区域，在题中有 3 个 VLAN，也就有 3 个广播域。

2. 解：AD

题目问：哪两个语句描述了思科 VLAN 的执行（选两个）？在默认情况下，交换机上只有 VLAN 1，交换机上所有端口都属于 VLAN 1，CDP、VTP 等控制信息也是在 VLAN 1 上传输的。在默认情况下，交换机的管理 IP 地址配置在 VLAN 1 上，VLAN 1002~1005 被自动创建，且不能修改。综上所述，A 和 D 的叙述正确，可以使用“show vlan”命令查看一个交换机的出厂配置，显示如下：


```
Switch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

3. 解: B

题目问: 参照图, 网络管理员不能远程连接到设备执行一个控制台会话。管理员执行“show ip interface brief”命令, 显示如图所示, 为什么远程连接失败? 从输出中可以看到 VLAN 1 被关闭, 从远程连接 192.168.1.100 这个管理 IP 地址自然是失败的。

4. 解: AD

题目问: 参照图, 关于交换机端口的配置, 哪两个语句是正确的? 交换机上的 Fa0/0 端口默认属于 VLAN 1, 图中的命令静态分配这个交换机端口到 VLAN 2。A 选项说交换机端口只属于 VLAN 2, 正确; B 选项说 Fa0/0 端口既属于 VLAN 1, 也属于 VLAN 2, 错误, 一个交换机端口不能同时属于两个 VLAN; C 选项说 Fa0/0 端口被动态映射到 VLAN 2, 错误, 图中是静态分配; D 选项说主机可以被连接到这个接口, 这是一个接入端口, 可以直接连接计算机, 正确。

5. 解: CF

题目问: 参照图, 一个网络助手需要配置图中的交换机和路由器, 使 VLAN 3 和 VLAN 4 中的计算机可以访问 VLAN 2 中的企业服务器, 哪两个以太网分段需要被配置成主干链路? 图中要实现的是 VLAN 间路由, VLAN 3 和 VLAN 4 中的计算机借助路由器提供的单臂路由功能来访问 VLAN 2 中的服务器, C (交换机与交换机之间) 和 F (交换机和路由器之间) 链路都需要被配置成主干链路来传输多个 VLAN 的信息。

6. 解: B

题目问: 当在 2950 交换机上配置一条新的主干链路时, 在默认情况下, 哪个 VLAN 允许在主干上传输? 在 Trunk 上默认是可以转发所有的 VLAN 数据的。

7. 解: A

题目问: 当在交换机上配置主干链路时, 哪个 VLAN 允许在主干上传输? 与上题类似, 在默认情况下, 主干链路上可以传输所有的 VLAN。

8. 解: BCD

题目问: 交换机有哪几种端口模式可以被用于主干? 可以参照本章的 10.2.4 节, 将链路配置为 Trunk 模式可以通过几种协商模式来完成: auto、desirable、on; 也可以通过静态指定 Trunk 来强制一条链路为 Trunk。

9. 解: B

题目问: 在思科 Catalyst 交换机上, “switchport trunk native vlan 999”命令的作用是什么

么？可以参照本章的 10.3.3 节，Native（本地）VLAN 是不打标签的 VLAN，题目中的命令指定本地 VLAN 为 999，主干端口对 VLAN 999 不打标签。

10. 解：CF

题目问：公司的 IP 电话和办公用的计算机都连在相同的设备上，为了确保语音数据流的最大吞吐量，公司需要确保语音流量和办公流量在不同的网络，最好用什么设备来直接连接电话和计算机？在这个设备上配置什么技术？参照本章 10.3.4 节，最好的网络设备当然是交换机了，然后利用交换机上语音 VLAN 功能来区分语音流和数据流。

11. 解：A

参照图：网络管理员已经在 Switch1 上创建了新的 VLAN 3，用来连接主机 C 和主机 D，网络管理员也正确地配置了 Fa0/13 到 Fa0/24 属于 VLAN 3，然而，网络管理员配置完成后，主机 A 可以和主机 B 进行通信，但不能和主机 C 或主机 D 进行通信，什么命令用来解决这个问题？可以参照本章的 10.4.2 节，这是一个多 VLAN 间通信的问题，虽然都同在一台交换机上，但是由于处在不同的 VLAN 中，而导致了不同 VLAN 中的主机是不能通信的。因此需要借助路由器的路由功能来实现不同 VLAN 间的通信，可以将 VLAN 中主机的网关指定为路由器与该 VLAN 相连的子接口的地址，这样 VLAN 间的数据包就都会发往网关，而由网关来进行进一步的转发。从图中可以看到，路由器上缺少 192.168.3.0 的子接口和 IP 地址，所以需要在路由器上添加一个子接口，封装 VLAN 3，并给其分配 192.168.3.0/24 网段中的 IP 地址。

12. 解：BD

题目问：图中的网络有连接问题，下面的哪个选项可以改正这个问题？主机 A 属于 VLAN 1，主机 A 的 IP 地址所在网段和路由器对应 VLAN 1 的子接口 Fa0/0.1 的 IP 地址所在网段是相同的；而主机 B 属于 VLAN 2，主机 B 的 IP 地址所在网段和路由器对应 VLAN 2 的子接口 Fa0/0.2 的 IP 地址所在网段是不同的，主机 B 处在 VLAN 2 中，主机 B 的网关 10.1.1.254 在 VLAN 1 中，主机 B 和网关之间的通信都是失败的，更别想访问其他网络了。因为路由器对应 VLAN 2 的子接口 Fa0/0.2 的 IP 地址是 10.1.2.254/24，所以应该给主机 B 也分配一个 10.1.2.0/24 的地址，并且网关要指向路由器 Fa0/0.2 的地址。

13. 解：D

题目问：参照图，在同一个 VLAN 内的主机可以通信，但在不同 VLAN 上的主机间不可能通信，为了允许 VLAN 间通信，需要做什么？同一交换机上的不同 VLAN 间的通信，必须借助于三层的接口，可以在交换机上接一个路由器，利用路由器的子接口和交换机之间做 Trunk，这样来实现连通性。

14. 解：DF

题目问：参照图，关于图中显示的 VLAN 间路由，哪两个语句是正确的（选两个）？A 选项说主机 A 和主机 F 使用相同的网关地址，该说法是错误的，主机 A 和主机 F 属于不同的 VLAN，不同的 VLAN 属于不同的子网，两个不同子网的主机网关不可能相同；B 选项说路由器 1 和交换机 2 将被使用一根交叉线相连，路由器和计算机属于同类设备，交换机和集线器属于同类设备，路由器和交换机属于不同类设备，不同类设备使用直通线相连，

同类设备才使用交叉线相连；C 选项说路由器 1 在主机 A 和主机 D 的通信中不起作用，该选项也是错误的，主机 A 和主机 D 属于不同的 VLAN，它们之间的通信要借助路由器来实现 VLAN 间路由；D 选项说路由器 1 的 Fa0/0 接口必须被配置子接口，该说法正确，配置路由器的子接口来实现 VLAN 间路由，每个子接口可以对应一个 VLAN；E 选项说路由器需要多个局域网接口来满足图中多个 VLAN 通信的需要，该说法不正确，通过使用子接口，路由器的一个物理接口即可满足要求；F 选项说路由器 1 的 Fa0/0 接口和交换机 2 的连接口必须使用相同的封装协议，这个说法是正确的，Trunk 的标准封装协议是 dot1Q，思科私有的封装协议是 ISL，现在多数厂家包括思科都默认使用 dot1Q 封装协议。

15. 解：ACF

题目问：参照图，网络管理员增加两台主机连接到交换机，哪三个选项可以被用来配置这些主机？看路由器上子接口的配置：接口 fa0/0.1 封装了 Trunk，并被划分到 VLAN 1 中，接口 fa0/0.10 封装了 Trunk，并被划分到 VLAN 10 中，接口 fa0/0.20 封装了 Trunk，并被划分到 VLAN 20 中。接下来看交换机上的接口的 VLAN 分配：和 host A 相连的接口 f0/6 划分到了 VLAN 10，而和 host B 相连的接口 f0/9 划分到了 VLAN 20。因为只有相同 VLAN 中的数据才可以通信，所以我们应该将 host A 的地址和 f0/0.10 配置一样的网段，而将 host B 的地址和 f0/0.20 配置一样的网段。并且因为主机是没有路由功能的，我们需要给它们指定网关，而它们的网关地址应该是相应 VLAN 中路由器的子接口的地址。所以，host A 的地址为 192.168.1.64~192.168.1.95，但要除了 192.168.1.78（该地址已经被分配给路由器接口，也就是默认网关）、192.168.1.64（是子网网络地址）、192.168.1.95（是子网广播地址）。host B 的地址为 192.168.1.128~192.168.1.191，但要除了 192.168.1.130（该地址已经被分配给路由器接口，也就是默认网关）、192.168.1.128（是子网网络地址）、192.168.1.191（是子网广播地址）。

16. 解：D

题目问：参照图，网络管理员评价当前网络设计的效率，RIPv2 在所有的三层设备上被使用，从 10.10.1.7 主机传输数据到 10.20.1.6 文件服务器，从源到目的经过设备的顺序是什么？PC 和文件服务器在不同的 VLAN 中，VLAN 间的通信需要经过路由器，图中并没有配置路由器的子接口，使用的是物理接口。PC 需要把数据包发往网关，也就是路由器的接口，PC 和路由器 Router1 的接口在同一个子网中，PC 的网关是 Router1 接口的 IP 地址。同样可以看出，文件服务器的网关是 Router2 的接口。从 PC 到服务器的流量应该是：PC 把去不同网段的数据包发往 Switch1，然后到达 PC 的网关 Router1，Router1 查询路由表，把数据包发往 Router2，Router2 再经过 Switch2 发往文件服务器。

第 11 章

VTP**

本章介绍 VTP 的相关操作，包括 VTP 的作用、特点、默认信息、域名、通告、模式和裁剪，并演示 VTP 的配置和排错。



11.1 VTP 介绍***

Cisco 交换机上一旦通过某种方式激活了干线，这些交换机会使用通告报文来指示哪些 VLAN 是可用的，并且会维持这些 VLAN 的相关信息，这项功能称为 VLAN 中继协议 (Vlan Trunking Protocol，简称 VTP)。VTP 是 Cisco 私有协议。

11.1.1 VTP 的作用***

VTP 负责在 VTP 域内同步 VLAN 信息，这样就不必在每个交换机上配置相同的 VLAN 信息。比如在一个有几十台交换机的企业网中，有十几个部门存在，需要在所有的交换机上都配置十几个 VLAN，工作量较大，且容易出错。可以使用 VTP 协议，把一台交换机配成 VTP Server，并配置相应的 VLAN，把其余的交换机配成 VTP Client，使它们可以自动学习到 Server 上 VLAN 信息。

VTP 在一组交换机之间进行 VLAN 通信，VTP 从一个中心控制点开始，维护整个企业网上 VLAN 的添加、删除和重命名工作，确保配置的一致性，将进行变动时可能会出现配置不一致性降至最低。

11.1.2 VTP 的特点***

VTP 是一种消息协议，使用第 2 层帧，通过 VLAN1 传输，在全网的基础上管理 VLAN 的添加、删除和重命名，以实现 VLAN 配置的一致性。可以用 VTP 管理网络中 VLAN 的范围从 1 到 1005，VTP 不能管理扩展的 VLAN (VLAN 号大于 1005)。

VTP 协议使用 VTP 通告 (VTP advertisements) 在交换机间交互 VLAN 信息，VTP 通告只能在 Trunk 链路上交互，也就是说，如果交换机之间的链路是 Access 链路，VTP 将不能通告 VLAN 的配置信息。

11.1.3 默认 VTP 信息**

运行 Packet Tracer 模拟器，打开光盘中的“配置\11\ntp.pkt”拓扑文件，拓扑中几台交换机的连接如图 11-1-1 所示。

使用 “show vtp status” 命令查看交换机 SW1 的 VTP 信

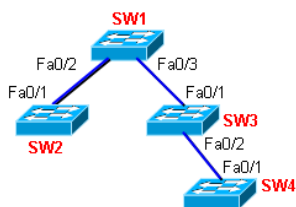


图 11-1-1 VTP 实验拓扑

息，显示如下：

```
SW1#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode          : Server
VTP Domain Name             :
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

上面显示的是思科多数交换机的默认 VTP 信息。

- “VTP Version: 2”，表示思科 2960 交换机上支持两种 VTP 的版本，即 Version 1 和 Version 2，默认运行的是 Version 1。
- “Configuration Revision: 0”，表示交换机的配置修正号是 0，当交换机的 VLAN 配置信息发生改变时，该值会被加 1，配置修正号的值暗示了交换机 VLAN 配置信息的新旧。稍后演示配置修正号在同步 VLAN 信息时的作用。
- “Maximum VLANs supported locally: 255”，表示该交换机上最大可以配置 255 个 VLAN，这个值与交换机的型号有关。
- “Number of existing VLANs: 5”，表示交换机上当前存在 5 个 VLAN，即默认存在的 VLAN 1 和 1002、1003、1004、1005。
- “VTP Operating Mode: Server”，表示 VTP 的模式是 Server（服务器），VTP 的模式还可以是 Client（客户端）或 Transparent（透明），VTP 的模式稍后介绍。
- “VTP Domain Name:”，表示 VTP 的域名为空，稍后介绍 VTP 的域名。
- “VTP Pruning Mode: Disabled”，表示没有使用 VTP 的裁剪，稍后介绍 VTP 的裁剪操作。
- “VTP V2 Mode: Disabled”，表示没有使用 VTP 的 V2，即默认使用的是 Version 1。为了 VTP 可以正常工作，同一个 VTP 域中所有交换机的 VTP 版本要一致。可以使用下面的命令修改 VTP 使用的版本：

```
SW1(config)#vtp version 1 或 2
```

- “VTP Traps Generation: Disabled”，Trap 主要用来为 SNMP 服务器发送消息，默认不使用，CCNA 中不涉及 Trap。
- “MD5 digest”，表示从 VTP 信息计算得出的散列值，如果 VLAN 信息发生改变，该散列值也随之改变。
- “Configuration last modified”，表示最后配置改变的时间。
- “Local updater ID is”，表示发送 VTP 消息的端口 IP 地址，可以指定发送 VTP 消息的端口，模拟器上不支持该操作，CCNA 考试中也不涉及。

11.1.4 VTP 域名（Domains）**

有了 VTP，就可以在一台交换机上集中进行配置了，所做的配置会被自动传播到网络中所有其他交换机上，但前提是所有的交换机必须工作在同一个 VTP 域中。为了让一台交换机可以向其他交换机传播 VTP 信息，该交换机必须要有一个 VTP 域名，在默认情况下，

交换机的域名为空。在同一个域中的交换机共享它们的 VLAN 信息，并且，一个交换机只能加入一个 VTP 域中，不同域中的交换机不能交换 VTP 信息。

配置图 11-1-1 中所有交换机之间的链路为主干链路，各交换机的配置命令如下：

```
SW1(config)#int fa 0/2
SW1(config-if)#swi mode trunk
SW1(config-if)#int fa 0/3
SW1(config-if)#swi mode trunk

SW2(config)#int fa 0/1
SW2(config-if)#swi mode trunk

SW3(config)#int fa 0/1
SW3(config-if)#swi mode trunk
SW3(config-if)#int fa 0/2
SW3(config-if)#swi mode trunk

SW4(config)#int fa 0/1
SW4(config-if)#swi mode trunk
```

在交换机 SW1 上新建 VLAN 2，然后使用“show vtp status”命令查看交换机的 VTP 信息，执行和显示如下：

```
SW1(config)#vlan 2
SW1(config-vlan)#end
SW1#show vtp status
VTP Version                : 2
Configuration Revision      : 1
Maximum VLANs supported locally : 64
Number of existing VLANs    : 6
VTP Operating Mode          : Server
VTP Domain Name             :
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x86 0x77 0xBF 0x40 0x39 0x85 0x09 0xED
Configuration last modified by 0.0.0.0 at 3-1-93 00:30:01
Local updater ID is 0.0.0.0 (no valid interface found)
```

从上面的输出中，可以观察到 SW1 的配置修正号已经变成了 1，因为 VLAN 的配置信息发生了变化，该值被从 0 增加到 1。已经存在的 VLAN 数也从 5 个增加到 6 个。

使用“show vtp status”命令查看 SW2、SW3、SW4 的 VTP 配置信息，发现没有任何变化，这是因为虽然 SW1 的配置信息发生了变化，但 SW1 的域名为空，SW1 不向外传播 VTP 通告。

使用下面的命令更改 VTP 的域名：

```
SW1(config)#vtp domain ccna
```

再次使用“show vtp status”命令查看交换机 SW1 的 VTP 信息，显示如下：

```
SW1#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 64
Number of existing VLANs    : 6
VTP Operating Mode          : Server
VTP Domain Name             : ccna
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x92 0x70 0xE6 0xEA 0xF3 0x3A 0x99 0x59
Configuration last modified by 0.0.0.0 at 3-1-93 00:30:01
Local updater ID is 0.0.0.0 (no valid interface found)
```

从上面的输出中，可以发现 VTP 的域名已经从空名字变成了“ccna”，注意 VTP 的配置修正号变成了“0”。当删除 VLAN 配置文件 vlan.dat 并重启交换机或更改 VTP 域名时，VTP 的配置修正号被自动清零。当交换机处在 Transparent 模式时，因为不需要与其他交换机同步 VTP 信息，配置修正号始终为 0。

使用“show vtp status”命令查看 SW2、SW3、SW4 的 VTP 配置信息，显示如下：

```
SW2#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 64
Number of existing VLANs    : 5
VTP Operating Mode          : Server
VTP Domain Name             : ccna
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xE1 0x2A 0x13 0xE5 0xB3 0xA4 0x96 0xA4
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

注意在上面的输出中，VTP 的域名已经变成了“ccna”，但存在的 VLAN 仍然是 5 个，并没有与 SW1 同步。出现这种现象，是因为 SW1 配置域名后开始向外发送通告，域名为空的交换机可以接收新的域名（如果是域名不一样，则不会自动更换域名），SW2、SW3、SW4 的域名都更改成 ccna。但因为 4 台交换机的配置修正号都是 0，它们之间不会同步 VLAN 的配置信息。

在 SW1 上再新增一个 VLAN 3，查看 SW1 的 VTP 信息显示如下：

```
SW1#show vtp status
VTP Version                : 2
Configuration Revision      : 1
Maximum VLANs supported locally : 64
Number of existing VLANs    : 7
VTP Operating Mode          : Server
VTP Domain Name             : ccna
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x53 0x59 0x95 0x9B 0x47 0xFF 0xBC 0x5C
Configuration last modified by 0.0.0.0 at 3-1-93 01:01:31
Local updater ID is 0.0.0.0 (no valid interface found)
```

SW1 的配置修正号从 0 变成了 1，存在的 VLAN 数也变成 7 个。

在 SW2、SW3 或 SW4 上查看 VTP 信息，显示如下：

```
SW2#show vtp status
VTP Version                : 2
Configuration Revision      : 1
Maximum VLANs supported locally : 64
Number of existing VLANs    : 7
VTP Operating Mode          : Server
VTP Domain Name             : ccna
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x53 0x59 0x95 0x9B 0x47 0xFF 0xBC 0x5C
Configuration last modified by 0.0.0.0 at 3-1-93 01:01:31
Local updater ID is 0.0.0.0 (no valid interface found)
```

从上面的输出中，可以看出 SW2 交换机的配置修正号也变成了 1，存在的 VLAN 也是 7 个，域名仍是 ccna，由 VLAN 信息计算出来的 MD5 散列值与 SW1 的完全相同，可以在 SW2

上使用“show vlan”命令，查看 SW2 上的 VLAN 配置，与 SW1 上的 VLAN 相同。

从上面的实验中，可以看到只要 VTP 域名相同，配置修正号大的交换机可以覆盖配置修正号小的交换机上的 VLAN 配置，这在实际工程中将会很不安全。工程中为了保护 VTP 域的安全，一般除了设置域名外，还配置 VTP 的域密码，只有域名和密码都相同的情况下，VTP 才会交互 VLAN 配置信息。配置 VTP 域密码的命令如下：

```
SW1(config)#vtp password cisco
```

11.1.5 VTP 通告 (Advertising) *

VTP 通告有时也被称为 VTP 消息 (Message)。

1. VTP 帧结构

VTP 帧被封装在 802.1Q 或 ISL 的帧中，VTP 帧以组播的方式发送，目的 MAC 地址是保留的 MAC 地址“01-00-0C-CC-CC-CC”。

VTP 帧包括帧头和信息内容。

- VTP 帧头中包括这些字段：域名、域名长度、VTP 版本、VTP 配置修正号、VTP 信息类型等。其中，VTP 信息的类型有 3 种，即汇总 (Summary)、子集 (Subnet)、查询 (Request)。
- VTP 信息内容包括 MD5 散列值、帧的格式 (ISL 或 802.1Q)，以及每一个 VLAN 的配置信息。每个 VLAN 的配置信息包括：VLAN ID、VLAN 名称、VLAN 类型 (如普通 VLAN 或语音 VLAN)、VLAN 的状态 (如激活或挂起)、VLAN 相关的其他信息等。

2. VTP 通告类型

VTP 通告有 3 种类型。

(1) 汇总通告 (Summary Advertisements)

汇总通告包括 VTP 的域名、配置修正号和 VTP 配置的一些细节。VTP 汇总通告采用周期性发送和触发更新的方式。周期性发送：每 5 分钟被 VTP Server 或 VTP Client 发送，用来通知工作在同一个域中的 VTP 邻居交换机，当前 VTP 配置修正号是多少。触发发送：如果 VTP 配置发生变化，VTP 汇总通告被立即发送。

(2) 子集通告 (Subset Advertisements)

子集通告包括具体的 VLAN 配置信息，在完全更新中，有时可能会发送多个子集通告。下面的这些变化会触发子集通告：

- 创建或删除 VLAN；
- 挂起或激活 VLAN；
- 改变 VLAN 的名字；
- 改变 VLAN MTU (Maximum Transmit Unit，最大传输单元)。

(3) 查询通告 (Request Advertisements)

当 VTP Server 收到一个查询通告时，VTP Server 会发送一个 VTP 汇总通告和一个 VTP 子集通告。在下列情况下，会发送查询通告：

- VTP 域名发生改变；
- 交换机收到一个汇总通告，汇总通告中的配置修正号高于本交换机的配置修正号；

- 因为某些原因，子集通告丢失；
- 交换机重启。

11.1.6 VTP 模式 (Modes) ***

思科交换机可以被配置成 3 种 VTP 模式,即 Server(服务器)、Client(客户)和 Transparent(透明)。

(1) Server 模式

工作在 Server 模式下的交换机,可以创建、修改、删除 VLAN。Server 模式是思科交换机的默认 VTP 模式。VTP Server 交换机通告自己的 VLAN 信息给同一个域中的其他交换机,同时也与收到的 VTP 通告同步 VLAN 信息。VLAN 的配置信息保存在 vlan.dat 文件中,删除 vlan.dat 文件重启后,交换机 VTP 恢复到出厂配置。

(2) Client 模式

工作在 Client 模式下的交换机,不可以创建、修改、删除 VLAN。当工作在 Client 模式下的交换机重启时,它发送一个查询通告给 VTP Server,请求更新的 VLAN 信息。VTP Client 交换机通告自己的 VLAN 信息给同一个域中的其他交换机,同时也与收到的 VTP 通告同步 VLAN 信息。VLAN 的配置信息保存在 vlan.dat 文件中,删除 vlan.dat 文件重启后,交换机 VTP 恢复到出厂配置。

在大型网络中,可以配置两台性能较好的交换机工作在 VTP Server 模式,配置两台的原因是为了起到冗余的作用。其他交换机工作在 VTP Client 模式,这样只需配置一台 Server 交换机的 VLAN 信息,全网中的交换机都可以同步 VLAN 配置,在 Client 的交换机上不能更改 VLAN 配置。

(3) Transparent 模式

工作在 Transparent 模式下的交换机,可以创建、修改、删除 VLAN,但所做的修改只影响当前的交换机。工作在 Transparent 模式下的交换机可以转发收到的 VTP 通告给网络中的其他交换机,但只是转发,Transparent 模式的交换机并不发送自己的 VTP 信息给其他交换机,也不与网络上的其他交换机同步 VLAN 信息。VLAN 的配置信息并不保存在 vlan.dat 中,而是保存在 running-config 中,如果想交换机重启后,仍然保存 VLAN 的信息,需要 copy running-config startup-config。删除 vlan.dat 文件,只要不删除 startup-config 文件,重启后,交换机的 VTP 模式和 VLAN 配置信息都不会发生改变。

表 11-1-1 对 VTP 的 3 种模式进行了对比。

表 11-1-1 VTP 的 3 种模式

	VTP Server	VTP Client	VTP Transparent
能否创建、修改和删除 VLAN	能	不能	能
能否发送 VTP 通告	能	能	仅能转发收到的 VTP 通告,不发送 VTP 通告
能否同步 VTP 信息	能	能	不能
VLAN 信息保存的位置	vlan.dat	vlan.dat	startup-config

11.1.7 VTP 裁剪 (Pruning) **

VTP Pruning 是 VTP 的一个功能,它能减少中继端口上不必要的信息量。在 Cisco 交换机上,VTP 裁剪功能默认是关闭的。

在默认情况下, 发送给某个 VLAN 的广播会通过主干链路传输到所有的交换机, 即使那台交换机上并没有位于相应 VLAN 的端口。在图 11-1-2 中, 在没有使用 VTP Pruning 的情况下, 假设 SW1 从 Fa1/4 端口收到一个广播帧, SW1 将从 Fa1/1 主干端口发送给 SW2, 尽管 SW2 上没有 VLAN 2 的端口。虽然最终 SW2 也会丢弃 VLAN 2 的广播包, 但还是浪费了 SW1 和 SW2 之间的链路带宽, 以及交换机的处理时间。

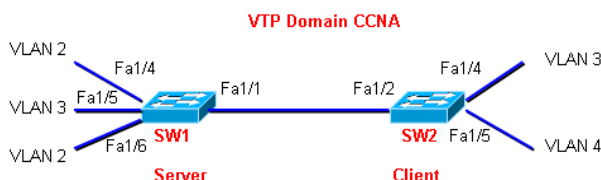


图 11-1-2 VTP 裁剪

在使用 VTP Pruning 的情况下, SW1 检测到 SW2 上没有 VLAN 2 的端口, SW1 将在 Fa1/1 端口上裁剪掉 VLAN 2 的流量, 同理, SW2 将在 Fa1/2 端口上裁剪掉 VLAN 4 的流量。

因为 Packet Tracer 中不支持 VTP Pruning (CCNA 考试中, 尤其是实验中, 不会出现这一内容), 这里改在 Dynamips 的 CCNA 机架上完成。开启 SW1 和 SW2, SW1 的配置如下:

```
Router>en
Router#conf t
Router(config)#host SW1
SW1(config)#exit
SW1#vlan data
SW1(vlan)#vtp domain CCNA
SW1(vlan)#vlan 2
SW1(vlan)#vlan 3
SW1(vlan)#vlan 4
SW1(vlan)#exit
SW1#conf t
SW1(config)#int fa 1/4
SW1(config-if)#swi mode acc
SW1(config-if)#swi acc vlan 2
SW1(config-if)#int fa 1/5
SW1(config-if)#swi mode acc
SW1(config-if)#swi acc vlan 3
SW1(config-if)#int fa 1/6
SW1(config-if)#swi mode acc
SW1(config-if)#swi acc vlan 2
SW1(config-if)#int fa 1/1
SW1(config-if)#swi mode trunk
```

VTP 域名是区分大小写的。

VTP 只能在主干上传输。

SW2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host SW2
SW2(config)#exit
SW2#vlan data
SW2(vlan)#vtp domain CCNA
SW2(vlan)#vtp client
SW2(vlan)#exit
SW2#conf t
SW2(config)#int fa 1/2
SW2(config-if)#swi mode trunk
SW2(config-if)#int fa 1/4
```

SW2 默认是 VTP Server, 这里把它改成 VTP Client。SW2 上不需要配置 VLAN, 当然处在 Client 模式下的交换机上也不能配置 VLAN, SW2 将可以从 SW1 上学到 VLAN 的编号和名称。

VTP 只能传输 VLAN 的相关信息, 并不能传输 VLAN 所属的端口信息。很多初学者都会有这种误解, 认为 SW2 将可以从 SW1 上学到 VLAN 的编号、名称, 以及每个 VLAN 所拥有的端口, 其实这种想法是错误的, 也是不合

理的。如果这种假设存在，VTP 域中所有交换机端口的 VLAN 分配都要一样，即使交换机上没有这个 VLAN 的用户，也要白白占用端口。

```
SW2(config-if)#swi mode acc
SW2(config-if)#swi acc vlan 3
SW2(config-if)#int fa 1/5
SW2(config-if)#swi mode acc
SW2(config-if)#swi acc vlan 4
```

SW1 和 SW2 配置完成后，稍后（因为主干链路要运行起来，VTP 的通告周期是 5 分钟。读者可以在主干链路运行起来后，修改 SW1 的 VLAN 配置信息，触发 VTP 通告）在 SW2 上查看 VLAN 信息，正确的显示如下：

```
SW2#show vlan-switch
```

VLAN	Name	Status	Ports
1	default	active	Fa1/0, Fa1/1, Fa1/3, Fa1/6 Fa1/7, Fa1/8, Fa1/9, Fa1/10 Fa1/11, Fa1/12, Fa1/13, Fa1/14 Fa1/15
2	VLAN0002	active	
3	VLAN0003	active	Fa1/4
4	VLAN0004	active	Fa1/5

使用 show interface trunk 查看 SW1 上的主干链路，显示如下：

```
SW1#show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa1/1	on	802.1q	trunking	1
Port	Vlans allowed on trunk			
Fa1/1	1-1005			
Port	Vlans allowed and active in management domain			
Fa1/1	1-4			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa1/1	1-4			

从上面的输出中，注意最后一行，提示 Fa1/1 上没有被裁剪掉的 VLAN 从 1 到 4，即所有的 VLAN 都不被裁剪。使用下面的命令启用 VTP 裁剪：

```
SW1(vlan)#vtp pruning
```

只需要在 VTP Server 上配置 VTP Pruning 就可以了，VTP Client 可以学习到 VTP Server 的配置。

配置完成后，再次查看 SW1 的主干链路，显示如下：

```
SW1#show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa1/1	on	802.1q	trunking	1
Port	Vlans allowed on trunk			
Fa1/1	1-1005			
Port	Vlans allowed and active in management domain			
Fa1/1	1-4			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa1/1	1,3-4			

从上面的输出中，可以看到 SW1 已经从 Fa1/1 端口上裁剪掉 VLAN 2 的信息。查看 SW2 的主干链路，显示如下：

```
SW2#show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa1/2	on	802.1q	trunking	1
Port	Vlans allowed on trunk			
Fa1/2	1-1005			
Port	Vlans allowed and active in management domain			
Fa1/2	1-4			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa1/2	1-3			

从上面的输出中，可以看到 SW2 已经从 Fa1/2 端口上裁剪掉 VLAN 4 的信息。



11.2 VTP 配置与排错**

本节介绍配置 VTP 的注意事项、VTP 的配置过程和 VTP 排错。

11.2.1 VTP 配置的注意事项**

配置 VTP 前，需要注意一些事项，对于初学者来说，遵循这些方面，可以减少 VTP 配置过程中错误的发生，确保可以成功地配置 VTP。

1. 配置 VTP Server

确认所有将要配置的交换机都恢复到默认设置。

配置交换机 VTP 域前，要重置交换机的 VTP 配置修正号。不重置配置修正号，将会对 VTP 域中的其他交换机产生潜在的干扰。

在网络中至少配置 2 台 VTP 服务器交换机。因为只有服务器交换机可以创建、删除和修改 VLAN。在首选 VTP 服务器交换机不可用的情况下，应该确保有一台备用 VTP 服务器。如果在网络中的所有交换机都配置在 VTP 客户端模式，将不能创建新的 VLAN。

首先配置 VTP 服务器，VTP 客户端将可以从主干链路上学到 VTP 配置信息。

- VTP 域名是区分大小写的，要确保 VTP 域中所有交换机的域名相同。
- 如果配置了 VTP 密码，要确保 VTP 域中所有交换机的 VTP 密码相同。如果 VTP 密码不同，交换机将拒绝接收 VTP 通告。
- 确保所有的交换机都配置为使用相同的 VTP 协议版本。VTP 版本 1 是不兼容 VTP 版本 2 的。在默认情况下，Cisco Catalyst 2960 交换机运行 VTP 版本 1，但能够运行 VTP 版本 2。
- 确保交换机之间的互连链路是主干链路。

2. 配置 VTP Client

与 VTP 服务器交换机配置一样，确认交换机当前的配置是默认配置。

- 配置 VTP 客户端模式。交换机默认工作在 VTP 服务器模式。
- 配置 Trunk。VTP 通告只能在主干链路上传输。
- 当连接到 VTP 域中时，需要一些时间来同步 VTP 信息。
- 验证 VTP 状态。配置端口前，确认已经学到正确的 VLAN 信息。
- 配置 Access 端口。当一个交换机工作在 VTP 客户端模式时，不能添加新的 VLAN，只可以分配端口到现有的 VLAN 中。

11.2.2 VTP 配置**

这里结合图 11-2-1 演示 VTP 的配置。图中 SW1 的 VTP 模式是 Server，SW2 和 SW4 的 VTP 模式是 Client，SW3 的 VTP 模式是 Transparent。PC1、PC2 和 PC3 都是 VLAN 3 中的计算机，它们的 IP 地址分别是 192.168.1.1/24、192.168.1.2/24、192.168.1.3/24。使用 VTP

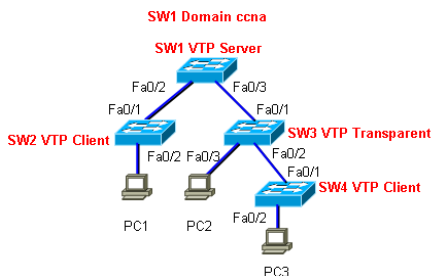


图 11-2-1 VTP 配置

配置图中的网络，使 3 台计算机之间可以通信。

运行 Packet Tracer 模拟器，打开光盘中的“配置\11\vtp 配置.pkt”拓扑文件。配置步骤如下：

（1）恢复所有交换机的配置到出厂配置

因为 4 台交换机使用的都是默认的出厂配置，这里可以省去该步骤。如果是工程中的交换机，需要使用“Switch#erase startup-config”命令删除启动配置文件，使用“Switch#delete vlan.dat”命令删除 VLAN 配置文件，然后再重启交换机。

（2）配置所有主干链路

将 4 台交换机之间的链路配置成主干链路。配置与 11.1.4 节中主干链路的配置相同，这里不再列出。

（3）配置 VTP Transparent

首先配置 SW3，因为该交换机的 VTP 模式是透明模式。

```
SW3(config)#vtp mode transparent 把VTP的模式设置成Transparent。
SW3(config)#vtp domain ccna      配置VTP域名为ccna,也可以配置成任意其他域名。
SW3(config)#vlan 3                添加VLAN3。
```

（4）配置 VTP Server 交换机

```
SW1(config)#vtp domain ccna      配置VTP域名。
SW1(config)#vlan 2                在VTP Server上添加VLAN。
SW1(config-vlan)#vlan 3
```

（5）配置 VTP Client 交换机

```
SW2(config)#vtp mode client      把VTP的模式设置成Client。
SW2(config)#vtp domain ccna      配置VTP域名为ccna。
Domain name already set to ccna. 提示域名已经是ccna了,这是因为域名已经与SW1同步了,配置域名这句可以省去。
```

```
SW4(config)#vtp mode client
```

（6）分配端口到对应的 VLAN

在 SW2 和 SW4 上，可以使用“show vtp status”命令查看 VTP 信息有没有与 SW1 同步，如果没有，请检查前面的配置步骤。SW2 和 SW4 与 SW1 同步后，可以使用“show vlan”命令检查 VTP Client 交换机上 VLAN 的信息，应该有后来添加的 VLAN 2 和 VLAN 3。

```
SW2(config)#int fa 0/2
SW2(config-if)#swi acc vlan 3
```

```
SW4(config)#int fa 0/2
SW4(config-if)#swi acc vlan 3
```

在 SW3 上，可以使用“show vtp status”命令查看 VTP 信息有没有与 SW1 同步，可以

发现并没有同步, 因为 SW3 的 VTP 工作在透明模式。使用 “show vlan” 命令检查 SW3 上的 VLAN 信息, 只有添加的 VLAN 3, 并没有 VLAN 2。工程中如果 SW4 上有 VLAN2 的用户, SW3 上必须添加 VLAN2, 否则 SW3 将不会在主干链路上转发不存在 VLAN 流量。

```
SW3(config)#int fa 0/3
SW3(config-if)#swi acc vlan 3
```

(7) 配置 PC1、PC2、PC3 的 IP 地址

(8) 测试

所有的 PC 之间都可以通信。配置完成。

11.2.3 VTP 排错**

在配置 VTP 过程中, 相关的错误有:

- **VTP 版本不一致。**思科 2960 交换机支持 VTP 版本 1 和 VTP 版本 2, 版本 1 和版本 2 是不兼容的, 可以使用 “show vtp status” 命令检查 VTP V2 Mode 是否显示的一致。
- **VTP 密码问题。**如果配置了 VTP 密码, 要确保同一个 VTP 域中, 所有 Server 和 Client 交换机的 VTP 密码都相同。
- **VTP 域名问题。**确保同一个 VTP 域中, 所有 Server 和 Client 交换机的 VTP 域名都相同, 域名是区分大小写的。
- **VTP 模式配置正确。**VTP 域中至少要有一台 VTP Server。
- **配置修正号问题。**要确保新加入 VTP 域中的交换机的配置已经恢复到出厂设置, 把配置修正号变成 0 后, 再加入 VTP 域中。

这里结合一个具体实例讲解 VTP 的故障排除。在图 11-2-2 中, 网络工作正常, PC1 和 PC2 之间可以正常通信。当把 Switch4 加入网络后, PC1 和 PC2 之间的通信失败。请读者找出原因所在。

运行 Packet Tracer 模拟器, 打开光盘中的 “配置\11\vtp 排错.pkt” 拓扑文件。在 PC1 上 ping PC2 的 IP 地址 192.168.1.2, 可以 ping 通。用一根交叉线把 Switch3 的 Fa0/2 端口和 Switch4 的 Fa0/1 端口连接起来, 这两个端口的主干链路都已配置过。此时测试 PC1 和 PC2 之间的连通性,

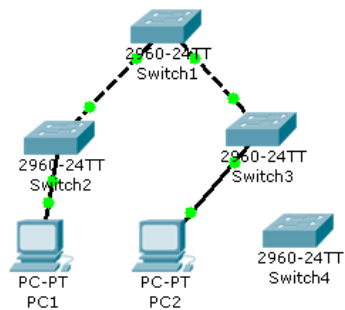


图 11-2-2 VTP 排错

仍然可以 ping 通, 等一段时间, 大约 5 分钟 (VTP 的更新周期), 模拟器上可能会需要更长的时间。读者也可以在 SW4 上使用 “SW4#debug sw-vlan vtp events” 命令, 监视 VTP 的事件, 当有事件发生时, 即可测试 PC1 和 PC2 之间的连通性, 结果 ping 失败。

读者关闭 Packet Tracer 模拟器, 不要保存, 再次打开光盘中的 “配置\11\vtp 排错.pkt” 拓扑文件。先不要连接 Switch3 和 Switch4 之间的连线, 查看 Switch1、Switch2、Switch3 和 Switch4 的 VTP 状态和 VLAN 配置信息, 查看 Switch2 和 Switch3 上 PC 所属的 VLAN 端口。显示如下:

```
SW1#show vtp status
VTP Version                : 2
Configuration Revision      : 1
Maximum VLANs supported locally : 64
Number of existing VLANs    : 6
VTP Operating Mode          : Server
VTP Domain Name              : ccna
```



```

VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0xCB 0xC7 0x93 0x48 0x03 0xD5 0xAF 0x58
Configuration last modified by 0.0.0.0 at 3-1-93 00:27:36
Local updater ID is 0.0.0.0 (no valid interface found)

```

```

SW4#show vtp status
VTP Version                : 2
Configuration Revision      : 13
Maximum VLANs supported locally : 64
Number of existing VLANs    : 6
VTP Operating Mode         : Client
VTP Domain Name            : ccna
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0xD5 0x78 0x26 0xAB 0x76 0x1A 0x33 0x17
Configuration last modified by 0.0.0.0 at 3-1-93 00:26:36

```

```

SW1#show vlan
VLAN Name      Status      Ports
-----
1    default    active    Fa0/1, Fa0/4, Fa0/5, Fa0/6
                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                Fa0/23, Fa0/24, Gig1/1, Gig1/2
2    VLAN0002    active

```

```

SW4#show vlan
VLAN Name      Status      Ports
-----
1    default    active    Fa0/1, Fa0/4, Fa0/5, Fa0/6
                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                Fa0/23, Fa0/24, Gig1/1, Gig1/2
100  VLAN0100    active

```

```

SW2#show vlan
VLAN Name      Status      Ports
-----
1    default    active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                Fa0/23, Fa0/24, Gig1/1, Gig1/2
2    VLAN0002    active    Fa0/2

```

然后连接 Switch3 和 Switch4 之间的连线，待 VTP 事件发生后（如果读者不想等 5 分钟左右的时间，可以配置 Switch1，随便添加一个 VLAN 8，触发 VTP 更新），再次查看 Switch1、Switch2、Switch3 和 Switch4 的 VTP 状态和 VLAN 配置信息。可以发现所有交换机上的 VTP 信息都与 Switch4 上的信息一致，因为 Switch4 有更高的 VTP 配置修正号，Switch4 上的 VLAN 信息覆盖了 Switch1、Switch2 和 Switch3 上的 VLAN 信息，造成网络的瘫痪。更为严重的是，这种错误很难被恢复，即使断开 Switch4 也不能恢复网络正常，解决办法只能是在 VTP Server 上重新添加以前的 VLAN，删除多余的 VLAN，如果之前没有文档记录，恢复起来很困难。

读者关闭 Packet Tracer 模拟器，不要保存，再次光盘中的打开“配置\11\vtp 排错.pkt”

拓扑文件。有了前面的经验教训，接下来重新把 Switch4 加入 VTP 域中。把 Switch4 加入 VTP 域中前，先使用下面的命令把 Switch4 的配置修正号恢复为 0。

```
SW4(config)#vtp domain test      更改 VTP 域名后，VTP 配置修正号恢复为 0。
SW4(config)#vtp domain ccna      把 VTP 域名重新改成正确的域名，但此时的配置修正号已经是 0。
```

此时再次查看 Switch4 的 VTP 信息，可以发现配置修正号已经调整到 0。把 Switch4 加入网络后，网络工作正常。



11.3 真题精选***

- What is the purpose of the Cisco VLAN Trunking Protocol?
 - to allow traffic to be carried from multiple VLANs over a single link between switches
 - to allow native VLAN information to be carried over a trunk link
 - to allow for managing the additions, deletions, and changes of VLANs between switches
 - to provide a mechanism to manually assign VLAN membership to switch ports
 - to provide a mechanism to dynamically assign VLAN membership to switch ports
- Which statement accurately describes a benefit provided by VTP?
 - VTP allows routing between VLANs.
 - VTP allows a single port to carry information to more than one VLAN.
 - VTP allows physically redundant links while preventing switching loops.
 - VTP allows switches to share VLAN configuration information.
- Which protocol provides a method of sharing VLAN configuration information between switches?
 - VTP
 - STP
 - ISL
 - 802.1Q
 - VLSM
- What is the purpose of the command shown below?
vtp password Fl0r1da
 - It is used to validate the sources of VTP advertisements sent between switches.
 - It is used to access the VTP server to make changes to the VTP configuration.
 - It allows two VTP servers to exist in the same domain, each configured with different passwords.
 - It is the password required when promoting a switch from VTP client mode to VTP server mode.
 - It is used to prevent a switch newly added to the network from sending incorrect VLAN information to the other switches in the domain.
- Refer to the exhibit. Given the output of the Floor3 switch, what statement describes the operation of this switch?

```
Floor3#show vtp status
VTP Version                : 2
Configuration Revision      : 1
Maximum VLANs supported locally : 250
Number of existing VLANs    : 8
VTP Operating Mode          : Client
VTP Domain Name             : XYZ
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
```

- A. VTP is disabled on this switch.
 - B. The switch can create, change, and delete VLANs.
 - C. The switch learns VLAN information but does not save it to NVRAM.
 - D. The switch can create VLANs locally but will not forward this information to other switches.
 - E. The switch learns VLAN information and updates the local VLAN data base in NVRAM.
6. Refer to the exhibit. The show vtp status command is executed at a switch that is generating the exhibited output. Which statement is true for this switch?

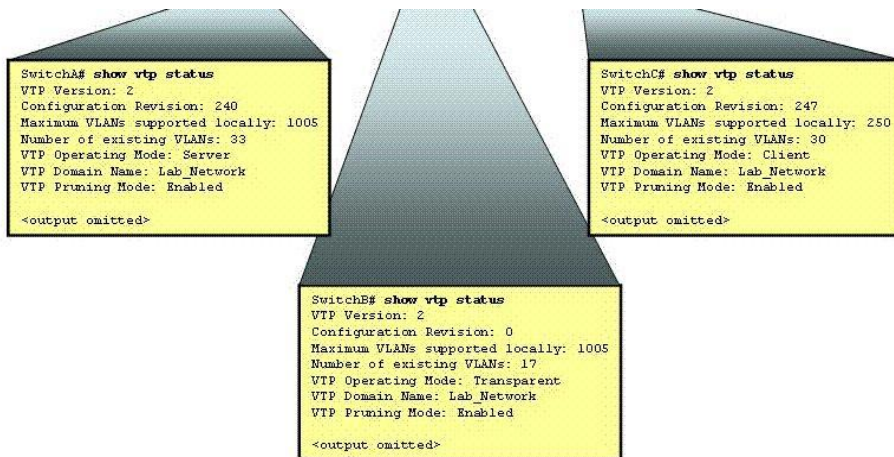
```
Switch# show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 64
Number of existing VLANs    : 17
VTP Operating Mode          : Transparent
VTP Domain Name             : ICND
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled

<output omitted>
```

- A. The switch forwards its VLAN database to other switches in the ICND VTP domain.
 - B. The configuration revision number increments each time the VLAN database is updated.
 - C. The switch forwards VTP updates that are sent by other switches in the ICND domain.
 - D. The VLAN database is updated when VTP information is received from other switches.
7. A network administrator has configured two switches, named London and Madrid, to use VTP. However, the switches are not sharing VTP messages. Given the command output shown in the graphic, why are these switches not sharing VTP messages?

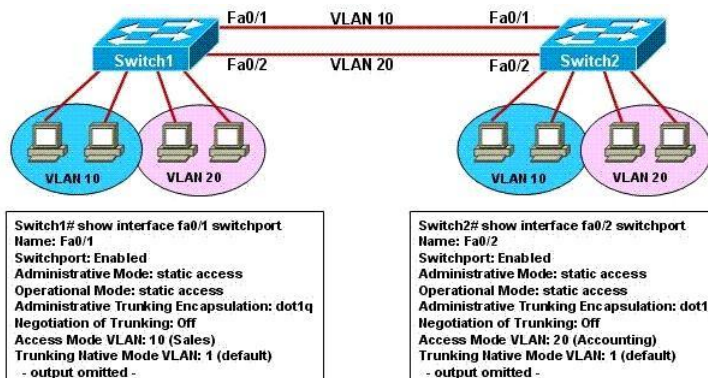
London# show vtp status		Madrid# show vtp status	
VTP Version	: 2	VTP Version	: 2
Configuration Revision	: 0	Configuration Revision	: 0
Maximum VLANs supported locally	: 64	Maximum VLANs supported locally	: 64
Number of existing VLANs	: 5	Number of existing VLANs	: 5
VTP Operating Mode	: Server	VTP Operating Mode	: Server
VTP Domain Name	: London	VTP Domain Name	: Madrid
VTP Pruning Mode	: Disabled	VTP Pruning Mode	: Disabled
VTP V2 Mode	: Disabled	VTP V2 Mode	: Disabled
VTP Traps Generation	: Disabled	VTP Traps Generation	: Disabled

- A. The VTP version is not correctly configured.
 - B. The VTP operating mode is not correctly configured.
 - C. The VTP domain name is not correctly configured.
 - D. VTP pruning mode is disabled.
 - E. VTP V2 mode is disabled.
 - F. VTP traps generation is disabled.
8. Refer to the exhibit. The network administrator has discovered that the VLAN configuration of SwitchC is not synchronized with the rest of the switched network. Why is SwitchC not receiving VTP updates?



- A. SwitchB is not relaying VTP advertisements to SwitchC.
- B. SwitchC has fewer existing VLANs than does SwitchA.
- C. SwitchA supports a greater number of VLANs than does SwitchC.
- D. SwitchC has a revision number higher than that being advertised.
- E. SwitchC should be operating in VTP server mode to receive VTP updates.
- F. SwitchB should be operating in VTP server or client mode to relay VTP updates.

9. Refer to the exhibit. An organization connects two locations, supporting two VLANs, through two switches as shown. Inter-VLAN communication is not required. The network is working properly and there is full connectivity. The organization needs to add additional VLANs, so it has been decided to implement VTP. Both switches are configured as VTP servers in the same VTP domain. VLANs added to Switch1 are not learned by Switch2. Based on this information and the partial configurations in the exhibit, what is the problem?



- A. Switch2 should be configured as a VTP client.
- B. VTP is Cisco proprietary and requires a different trunking encapsulation.
- C. A router is required to route VTP advertisements between the switches.
- D. STP has blocked one of the links between the switches, limiting connectivity.
- E. The links between the switches are access links.



11.4 真题解答***

1. 解：C

题目问：思科 VTP 协议的目的是什么？VTP 是 VLAN 中继协议，用来管理 VLAN 在交换机间添加、删除和修改。本章 11.1.1 节介绍了 VTP 的作用。这里强调的是 VTP 仅传输的 VLAN 的配置信息，并不传输 VLAN 中端口的成员信息，也就是说，VTP 可以让一个交换机从其他交换机学到有哪些 VLAN，至于每个 VLAN 中有哪些端口，还需要管理员手工配置。

2. 解：D

题目问：哪一个语句准确地描述了 VTP 提供的优点？VTP 允许交换机间同步 VLAN 的信息，共享 VLAN 的配置信息。

3. 解：A

题目问：哪一个协议提供了一种在交换机间共享 VLAN 配置信息的方法？本题的正确答案是 VTP。STP 是 Spanning Tree Protocol（生成树协议）的简写，STP 用来避免交换网络中的环路；ISL 是思科私有的 Trunk 链路封装协议，现在大多使用 dot1Q；802.1Q 是标准的 Trunk 链路封装协议，也就是 dot1Q；VLSM 是 Variable Length Subnet Masks（可变长度子网掩码）的简写，VLSM 主要用来高效地使用 IP 地址。

4. 解：A

题目问：“vtp password Fl0r1da”命令的作用是什么？VTP 密码是为了保证在同一个 Domain 里的交换机的安全，在同一个 Domain 里交换机只有域名和密码都相同才交互 VLAN 信息。可以参照本章的 11.1.4 节。

5. 解：C

题目问：参照图，给出了三层交换机的输出，哪一个语句描述了该交换机的操作？本题可以参照本章 11.1.6 节，从图中可以看到有关 VTP 的信息有：VTP 功能已经开启了，域名为 XYZ，模式为 Client。A 选项说交换机没用启用 VTP，错误；B 选项说这台交换机可创建、改变和删除 VLAN，Client 模式的交换机没有这样的功能；D 选项说这台交换机能够创建本地的 VLAN，但不转发 VLAN 信息到其他交换机上，这描述的是 Transparent（透明）模式的交换机；E 选项说这台交换机学习 VLAN 信息，更新本地在 NVRAM 中的 VLAN 数据库，Client 模式交换机的 VLAN 信息不保存在 NVRAM 中。只有选项 C 正确，Client 模式的交换机学习 VLAN 信息，但并不保存在 NVRAM 中，Transparent 模式交换机的 VLAN 配置信息保存在 NVRAM 中。

6. 解：C

题目问：参照图，在一台交换机上执行“show vtp status”命令，产生图中的输出，关于这台交换机的哪一个语句是正确的？VTP 是为了动态学习和同步 VLAN 信息的，但是它的同步和学习都是以域为单位的，只有同一个域中的 VLAN 信息才可以同步和学习。而 VTP 的模式有 3 种：Server、Client、Transparent。其中，Transparent 模式为透明模式，在这种模式下的 VLAN 信息是不能被其他设备学习到的，这种模式下的设备也不学习其他设备的

VLAN 信息，它只是转发 VLAN 信息，但是不学习。因为不需要与别的交换机同步配置，Transparent 模式交换机的配置修正号始终是 0。

7. 解：C

题目问：网络管理员配置了两台交换机使用 VTP，交换机的名字是 London 和 Madrid，然而交换机间不能共享 VTP 信息，给出图中的命令输出，为什么两台交换机不能共享 VTP 信息？交换机间不能共享 VTP 信息，就需要检查 VTP 的状态，首先需要检查的是 VTP 的域名，只有同一个域中的才可能相互学习，然而图中两台交换机的 VTP Domain 却是不一致的。

8. 解：D

题目问，参照图，网络管理员已经发现交换机 C 上的 VLAN 配置没有和网络中的其他交换机同步，为什么交换机 C 不接受 VTP 更新？首先看到交换机 B 是 Transparent 模式，该交换机不与其他交换机同步 VLAN 信息。交换机 A 和交换机 C 的 VTP 域名相同，一个是服务器，一个是 Client。交换机 C 之所以不同步交换机 A 的 VLAN 配置信息，是因为交换机 C 上有更高的配置修正号。解决的办法是更换交换机 C 的 VTP 域名或者删除 vlan.dat 文件，把配置修正号清零。

9. 解：E

题目问：参照图，一个组织连接两个站点，支持两个 VLAN 跨越两台交换机，不需要进行 VLAN 间通信。网络工作正常，并且全部被连接。这个组织决定使用 VTP 来增加额外的 VLAN，这两台交换机在同一个 VTP 域中都被配置成 Server，交换机 1 上增加的 VLAN 没有被交换机 2 学到。基于图中给出的部分配置信息，可能是什么问题？从图中的输出可以看到，两台交换机之间两根线缆都是接入线缆，分别属于 VLAN 10 和 VLAN 20，没有配置 Trunk，而 VTP 协议仅在 Trunk 链路上传输。

第 12 章

STP***

在分层网络中，管理员不得不通过冗余拓扑来保障网络的高可用性。然而，网络中额外添加的链路连接着路由器和交换机，会引起流量的环路。这些链路必须能被动态管理，当一个交换机的连接丢失时，另一条链路能快速地取代失败链路，并且不会产生新的流量环路。本章将讲述 STP（Spanning-Tree Protocol，生成树协议）如何在交换网络中解决环路问题，以及一些高级 STP 的工作方式。主要包括这样几个内容：冗余拓扑中存在的问题、生成树协议、生成树收敛、高级生成树协议。



12.1 冗余拓扑中存在的问题***

在图 12-1-1 中，PC1 和 PC3 之间可以通过 SW1 的 Fa1/1 和 SW2 的 Fa1/2 之间的链路连通，可是如果 SW1 和 SW2 之间的这条链路中断，将会导致 PC1 和 PC3 之间的通信中断。为了解决单一链路故障引起的网络问题，可以考虑在 SW1 和 SW2 之间再新增一条链路，如图 12-1-2 所示。

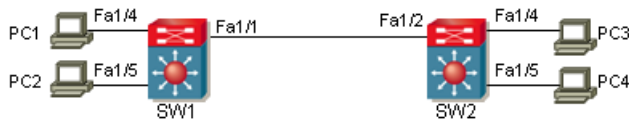


图 12-1-1 单一链路的拓扑

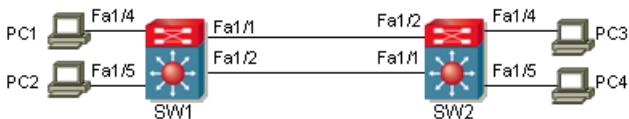


图 12-1-2 有冗余链路的拓扑

在图 12-1-2 中，SW1 和 SW2 之间任何一条链路的失败，将不会导致 PC1 和 PC3 之间的通信故障。冗余链路很好地解决了 SW1 和 SW2 之间单链路故障引起的网络中断，但在执行冗余拓扑前，有些问题必须考虑。

1. 广播风暴

以太网交换机传送的第二层数据帧不像路由器传送的第三层数据包有 TTL（Time To Live，生命周期），如果有环路存在，第二层的以太网帧不能被适当终止，它们将在交换机和交换机之间永无止境地传递下去，除非环路被破坏，否则将造成网络拥塞，甚至是网络

瘫痪。

前面介绍过交换机的工作原理，交换机收到一个广播帧，为了确保在同一个广播域中的所有设备都能收到这个广播帧，它将向除接收端口以外的所有端口转发这个广播帧。

下面来看一个广播风暴是如何形成的。在图 12-1-2 中：

- ① PC1 发出一个广播帧。
- ② SW1 收到这个广播帧，SW1 从 Fa1/1、Fa1/2、Fa1/5 端口向外转发这个广播帧。
- ③ SW2 从 Fa1/2 端口收到 SW1 从 Fa1/1 端口发过来的广播帧，然后 SW2 从 Fa1/1、Fa1/4、Fa1/5 端口把广播帧转发出去；SW2 从 Fa1/1 端口收到 SW1 从 Fa1/2 端口发过来的广播帧，然后 SW2 从 Fa1/2、Fa1/4、Fa1/5 端口把广播帧转发出去。
- ④ 同理，SW1 也从 Fa1/1 和 Fa1/2 端口接收到 SW2 转发过来的广播帧，然后从除接收端口之外的所有端口转发出去。
- ⑤ PC1、PC2、PC3、PC4 不停地接收到广播帧，根据广播帧的内容丢弃或处理广播帧。
- ⑥ 一个广播帧，在 SW1 和 SW2 间不停地被转发，永无止境，最终造成网络拥塞或瘫痪，影响网络正常使用。

2. MAC 地址表不稳定

广播风暴危害巨大，除了产生大量的流量之外，还会造成交换机的 MAC 地址表不稳定。在广播风暴的形成过程中：

- ① SW1 从 Fa1/4 端口接收到 PC1 的广播帧，SW1 根据帧的源 MAC 地址进行学习，记录下 PC1 的 MAC 地址在 Fa1/4 端口。SW1 把广播帧转发给 SW2。
- ② 假设 SW2 从 Fa1/1 端口先收到广播帧，SW2 记录下 PC1 的 MAC 地址在 Fa1/1 端口，然后 SW2 从 Fa1/2 端口也收到这个广播帧，SW2 更新 PC1 的 MAC 地址在 Fa1/2 端口。SW2 把接收到的广播数据帧再转发到 SW1。
- ③ SW1 先后从 Fa1/2 和 Fa1/1 端口接收 SW2 转发过来的广播帧，依次更新 PC1 的 MAC 地址在 Fa1/2 和 Fa1/1 端口。可真正的 PC1 在 Fa1/4 端口。
- ④ SW1 和 SW2 随着广播帧不停地被转发而不停地更换 MAC 地址表，造成 CPU 使用率过高，影响交换机的性能。

3. 重复帧拷贝

冗余拓扑除了带来广播风暴和 MAC 地址表不稳定外，还会引起重复帧拷贝问题。

- ① 假使 PC1 发出一个单播帧，目标是 PC3，SW1 收到这个单播帧，可 SW1 在 MAC 地址表中没有找到目标 PC3 的 MAC 地址，SW1 从除接收端口以外的所有端口把这个单播帧转发出去。
 - ② SW2 从 Fa1/1 端口收到 SW1 转发过来的单播帧，SW2 知道 PC3 接在 Fa1/4 端口，SW2 把这个单播帧仅从 Fa1/4 端口转发给 PC3，PC3 接收到这个单播帧。
 - ③ SW2 从 Fa1/2 端口收到 SW1 转发过来的单播帧，SW2 知道 PC3 接在 Fa1/4 端口，SW2 把这个单播帧只从 Fa1/4 端口转发给 PC3，PC3 再次接收到这个单播帧。
- PC1 仅发送一次单播帧，PC3 却收到两次。在工程中，重复帧拷贝也存在不足，比如在流量统计或计费软件的环境中，都造成不精确计算的问题。

实验：环路的判断

如何判断网络中出现环路了呢？直接的感觉就是网速很慢；直观的方法就是观察交换

机或集线器的指示灯；理性的分析应该是抓取数据包。这里用前面介绍过的 Sniffer 软件给大家演示环路判断。

① 构建网络拓扑。可以在计算机的前面加入一台集线器或不支持 STP 功能（也就是最便宜的）的交换机。如图 12-1-3 所示，用一根交叉的双绞线把设备的两个端口直接连接起来。

② 开始捕获包。在计算机上运行 Sniffer，单击“Start”按钮，开始抓包，如图 12-1-4 所示。

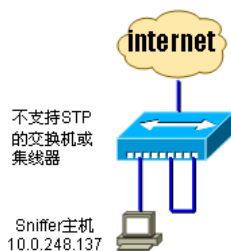


图 12-1-3 有环路的拓扑

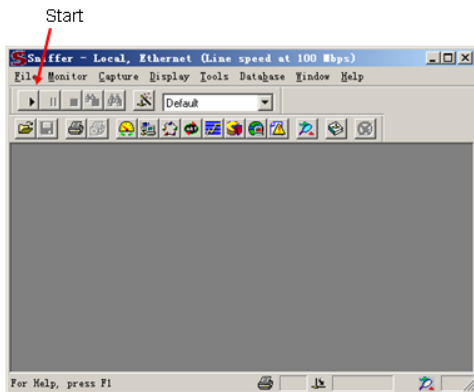


图 12-1-4 开始抓包

③ 制造出一个广播包。在实际的网络环境中，不需要制造也会有很多广播包，这里我们在计算机中制造出一个广播包。单击“开始”→“运行”，输入“cmd”后回车，打开 DOS 窗口。在 DOS 窗口中执行“arp -d”命令删除本机的 ARP 缓存，然后执行“ping 10.0.248.1”命令，ping 本机的网关，因为本机的 ARP 缓存表中没有网关 IP 地址对应的 MAC 地址，计算机会以广播形式发送 ARP 查询包，如图 12-1-5 所示。可一个应答也没有收到，这是因为网络已经产生了广播风暴。

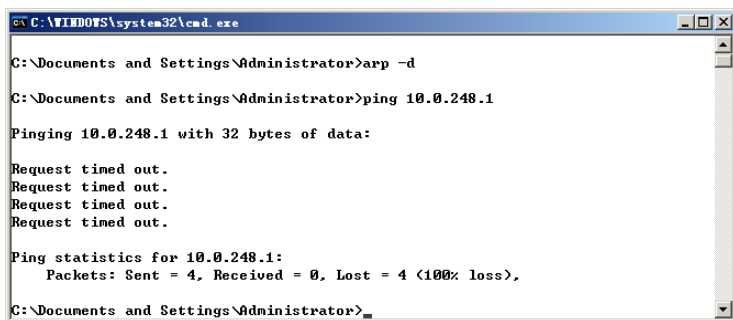


图 12-1-5 计算机发送 ARP 查询广播包

④ 停止捕获包。此时图 12-1-4 窗口中的“Stop and Display”按钮变得可操作，单击该按钮，停止捕获，如图 12-1-6 所示。

⑤ 显示捕获的包。停止捕获包后，显示如图 12-1-7 所示的窗口，单击窗口中的“Decode”标签。

⑥ 分析捕获的包。在打开的解码窗口中，如图 12-1-8 所示，滚动第一个子窗口中的滚动条，可以显示出捕获的包，可以发现其中有大量的 ARP 广播包，源地址来自同一个 MAC

地址。在第二个子窗口中可以发现，这是一个“ARP request”包，要解析的 IP 地址是“10.0.248.1”。

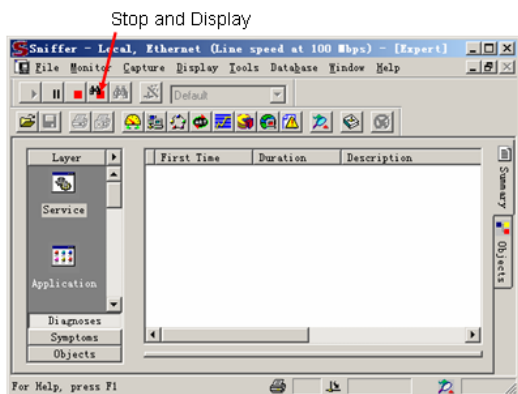


图 12-1-6 停止捕获包

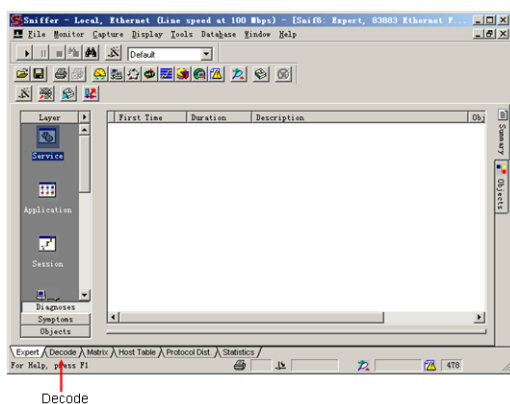


图 12-1-7 选择解码标签

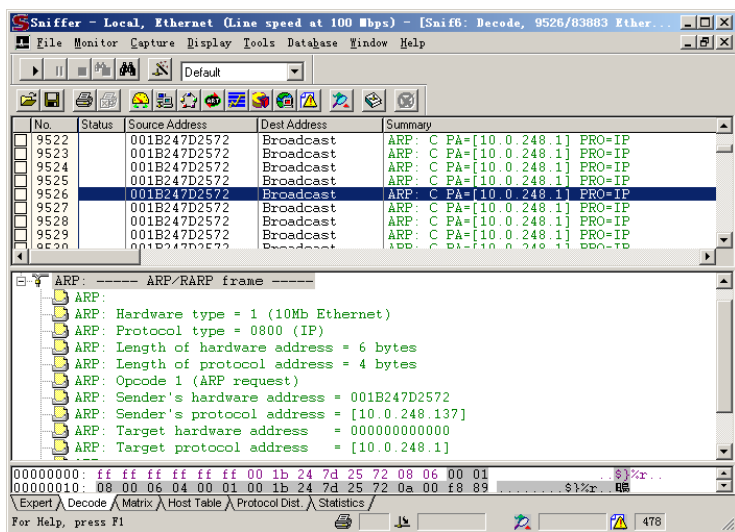


图 12-1-8 解码窗口

⑦ 解决环路。找到并断开网络中的二层冗余路径，或者启用 STP 协议。

生活中网卡或其他网络接口损坏、环路、人为干扰破坏、黑客工具、病毒传播，都可能引起广播风暴，交换机会把大量的广播帧转发到每个端口上，这会极大地消耗链路带宽和硬件资源。当出现网络异常时，不妨用 Sniffer 抓包，然后分析捕获数据包的特征，判断有没有出现二层环路。下一节讨论通过使用 STP 技术来有效地抑制广播风暴，避免网络拥塞。



12.2 STP 介绍***

通过冗余解决了由于单链路或单交换机故障引起的网络中断，提高了网络的可用性。当在第二层采用冗余时，又会带来广播风暴、MAC 地址不稳定、重复帧拷贝等问题，STP 被用来解决上述问题。

12.2.1 STP 算法***

STP 通过阻塞冗余路径上的一些端口，确保到达任何目标地址只有一条逻辑链路。处于阻塞状态的端口阻止网络流量的进入或离开，这里说的网络流量不包括 BPDU（Bridge Protocol Data Unit，桥接数据单元），STP 借助交换 BPDU 来阻止环路。在 STP 运行的情况下，虽然逻辑上没有环路，但物理路径仍然存在，只是被禁用以阻止环路发生，如果正在使用的链路或交换机出现故障，STP 重新计算，部分被阻止的端口被激活用来提供冗余。

STP 使用 STA（Spanning Tree Algorithm，生成树算法）决定交换机上的哪些端口被阻塞来阻止环路的发生。STA 选择一台交换机作为根交换机，也称根桥（Root Bridge），以该交换机作为参考点计算所有的路径。在图 12-2-1 中，所有交换机交换 BPDU，BPDU 中包括 BID（Bridge ID，桥 ID），BID 用来识别是哪台交换机发出的 BPDU。有关 BPDU 将在下一小节讨论。

1. 根交换机选举

BID 一般由 3 部分组成：优先级、发送交换机的 MAC 地址和 Extended System ID（扩展的系统 ID，可选项），如图 12-2-2 所示，共 8 个字节，其中，优先级 2 个字节，MAC 地址 6 个字节。

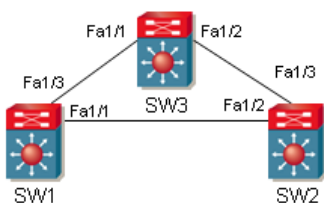


图 12-2-1 多交换机间的冗余拓扑

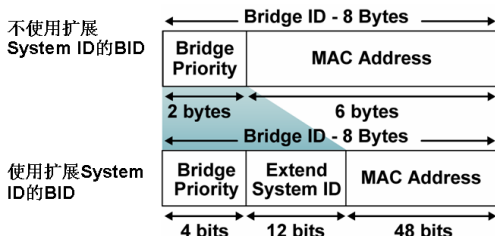


图 12-2-2 交换机的 BID

在不使用 Extended System ID 的情况下，BID 由优先级域和交换机的 MAC 地址组成，针对每个 VLAN，交换机的 MAC 地址都不一样，交换机的优先级可以是 0~65535。Dynamips 的 CCNA 模拟机架中的交换机不使用 Extended System ID，比如在 CCNA 机架中，交换机 SW1 中存在两个 VLAN：VLAN 1 和 VLAN 100，执行“show spanning-tree brief”（在很多新款的交换机、Packet Tracer 模拟器以及考试中使用的命令是 show spanning-tree）命令时，可以发现两个 VLAN 的 BID 优先级都是 32768，但 MAC 地址相差 1，一个是 cc00.0af4.0000，另一个是 cc00.0af4.0001，如图 12-2-3 所示。如果还存在 VLAN 200，则 MAC 地址是 cc00.0af4.0002。

在使用 Extended System ID 的情况下，每个 VLAN 的 MAC 地址可以相同，BID 被要求包含 VLAN ID 信息，解决的办法是从优先级域的 16 个 bit 中拿出低位的 12 个 bit，称为扩展的 System ID，用来唯一标识每个 VLAN 号，剩下的 4 个 bit 用来表示交换机的优先级，这种情况下优先级的取值只有 $2^4=16$ 个，是 4096 的倍数。想一想，为何从优先级中拿出的是 12 个 bit 来表示 Extended System ID 呢？原因是 ISL 封装中只有 10 个 bit 用于 VLAN 标识，802.1Q 封装中有 12 个 bit 用于 VLAN 标识，不管是哪种封装，取 12 个 bit 都可以满足。比如交换机优先级是 4096，交换机的 MAC 地址是 cc00.0af4.0000，交换机在 VLAN 100 中

的 BID 是 4196 (4096+100=4196) +cc00.0af4.0000。下面的输出来自思科 Catalyst 4503, 该交换机使用的 IOS 是 “cat4000-i9s-mz.122-25.EWA6.bin”。顺便提一下, Packet Tracer 模拟器中的交换机使用的是 Extended System ID。

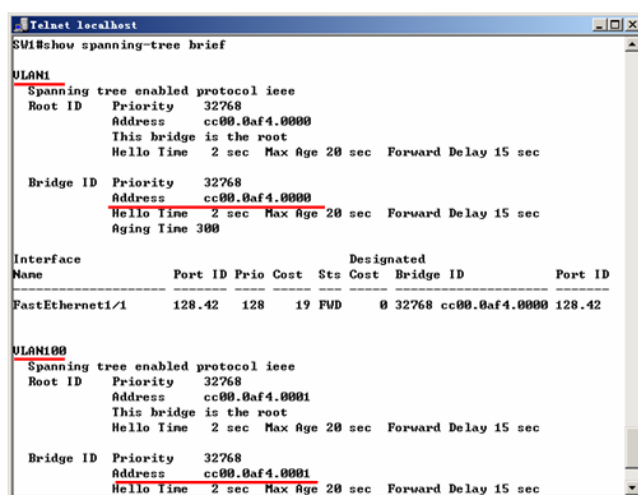


图 12-2-3 不使用 Extended System ID 的生成树

```
4503-2#show spanning-tree
```

```
VLAN0001
```

```
Spanning tree enabled protocol ieee
```

```
Root ID    Priority    20481
Address    0019.566e.1580
This bridge is the root
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Bridge ID  Priority    20481 (priority 20480 sys-id-ext 1)
Address    0019.566e.1580
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time  300
```

```
Interface    Role Sts Cost        Prio.Nbr Type
```

```
-----
Gi1/2        Desg FWD 4          128.2    P2p
Gi1/3        Desg FWD 4          128.3    P2p
```

```
VLAN0002
```

```
Spanning tree enabled protocol ieee
```

```
Root ID    Priority    24578
Address    0019.566e.1500
Cost       4
Port       2 (GigabitEthernet1/2)
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Bridge ID  Priority    28674 (priority 28672 sys-id-ext 2)
Address    0019.566e.1580
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time  300
```

```
Interface    Role Sts Cost        Prio.Nbr Type
```

```
-----
Gi1/2        Root FWD 4          128.2    P2p
Gi1/3        Desg FWD 4          128.3    P2p
```

```
VLAN0004
```

```

Spanning tree enabled protocol ieee
Root ID    Priority    24580
           Address     0019.566e.1500
           Cost        4
           Port        2 (GigabitEthernet1/2)
           Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec

```

```

Bridge ID  Priority    28676 (priority 28672 sys-id-ext 4)
           Address     0019.566e.1580
           Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time   300

```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Gil/2	Root	FWD	4	128.2		P2p
Gil/3	Desg	FWD	4	128.3		P2p

请注意该 4503-2 交换机 VLAN1、2、4 的 Address 都是“0019.566e.1580”，和图 12-2-3 中的不同，但所有 VLAN 的 BID 却不同，尤其是 VLAN 2 和 VLAN 4，尽管优先级设的都是 28672，但它们的 sys-id-ext 却分别是 2 和 4，VLAN 2 和 VLAN 4 的最终优先级是优先级加 sys-id-ext，结果 VLAN 2 的优先级是 28674，VLAN 4 的优先级是 28676。从上面的输出中，还可以看到 Type 是“P2p”，表示链路类型是点对点，这是快速生成树的特征，有关快速生成树，后面会介绍到。输出中“Spanning tree enabled protocol ieee”表示交换机使用的生成树协议是 PVST+，是思科交换机默认使用的生成树协议，后面会介绍到 PVST。

值得一提的是，现在普遍的交换机都使用 Extended System ID。拥有最小 BID 的交换机被选为根交换机。

在同一个广播域中的所有交换机参与选举根交换机。当一台交换机最初启动时，它假定自己就是根交换机，并发送“次优”BPDU，默认每 2 秒发送一个 BPDU 帧，BPDU 帧的 BID 和 Root ID（根交换机的 BID）相同。

在同一个广播域中的交换机相互之间转发 BPDU 帧，交换机从接收到的 BPDU 中读取 Root ID，如果读取到的 Root ID 比本交换机的 BID 小，交换机更新 Root ID 为邻居交换机的 Root ID，标识邻居交换机为根交换机。交换机继续转发更改过 Root ID 的 BPDU 帧到其他交换机，最后在同一个生成树实例中的所有交换机都有一致的 Root ID，也就是根交换机的 BID。

运行 CCNA 机架中的 SW1 和 SW3 交换机，两台交换机都没有使用扩展的 System ID，交换机 SW3 的 MAC 地址是 cc02.0af4.0000，交换机 SW1 的 MAC 地址是 cc00.0af4.0000，在 SW3 上执行“show spanning-tree brief”命令，查看 STP 根交换机的选举情况，如图 12-2-4 所示。

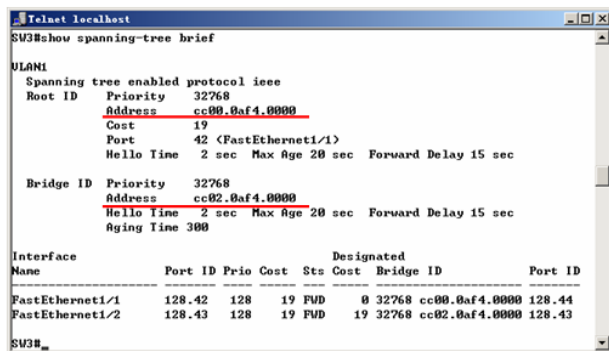


图 12-2-4 查看 STP 根交换机的选举情况

在图 12-2-4 中，可以看出针对 VLAN 1（在默认情况下交换机上只有 VLAN1），SW3 的 BID 是 32768（交换机的默认优先级）+cc02.0af4.0000，Root ID 是 32768+cc00.0af4.0000。BID 和 Root ID 不同，说明在 SW1 和 SW3 中，SW3 不是根交换机，SW1 是根交换机，因为 SW1 有更低的 BID，可以在 SW1 上使用 show 命令验证。

现在把 SW3 更改为 VLAN 1 的根交换机，因为在不使用 Extended System ID 的情况下，BID 由交换机的优先级和 MAC 地址组成，交换机的 MAC 地址固定，所以可以通过修改交换机的优先级实现。如下配置把交换机 SW3 的优先级降到 1000：

```
SW3(config)#spanning-tree vlan 1 priority ?
<0-65535> bridge priority
SW3(config)#spanning-tree vlan 1 priority 1000
```

如果是在使用 Extended System ID 的交换机上，优先级只能设成 0、4096、8192 等 4096 的倍数，因为在使用 Extended System ID 的交换机上，优先级只占用了高位的 4 个比特，低位的 12 个比特被 VLAN ID 占用。更改优先级后，SW3 的 BID 是 1000（交换机的默认优先级）+cc02.0af4.0000，小于 SW1 的 BID，SW3 将成为根交换机，如图 12-2-5 所示，结论得到验证。

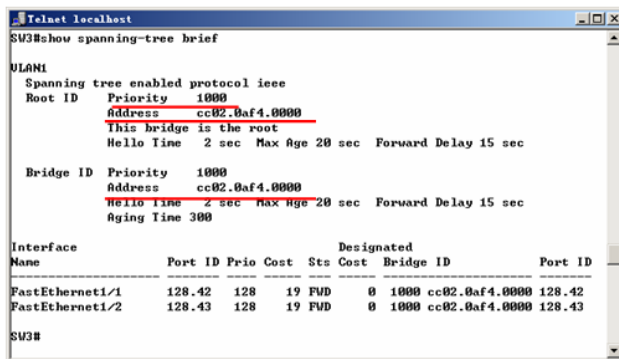


图 12-2-5 更改交换机的 BID

也可通过下面的配置来更改交换机的优先级：

```
SW3(config)#spanning-tree vlan 1 root ?
primary Configure this switch as primary root for this spanning tree
secondary Configure switch as secondary root
SW1(config)#spanning-tree vlan 1 root primary
% This switch is already the root of VLAN1 spanning tree
VLAN 1 bridge priority unchanged at 8192
VLAN 1 bridge max aging time unchanged at 20
VLAN 1 bridge hello time unchanged at 2
VLAN 1 bridge forward delay unchanged at 15
SW3(config)#
```

“spanning-tree vlan 1 root primary”是一个动态设置交换机优先级的命令。比如，网络中已经存在根交换机了，根交换机的优先级是 200，MAC 地址比该交换机的小，那么这条命令将可以把该交换机的优先级设置成 199，使该交换机成为新的根交换机。

2. 端口花费和路径花费

根桥被选举出来以后，计算其他交换机到根桥的花费，STA 考虑端口花费和路径花费。端口花费默认和端口带宽有关，但可以人为修改。路径花费等于从根交换机到达最终交换机前进方向上进入方向的端口花费总和，比如在图 12-2-1 中，SW1 是根交换机，想改变

SW3 到根交换机的花费，应该在 SW3 的 Fa1/1 端口改变花费，而不是在 SW1 的 Fa1/3 端口。如果一台交换机有多条路径可以到达根交换机，交换机选择路径花费最小的那条路径。

(1) **端口花费**。默认的端口花费与端口的速度有关，请参照表 12-2-1。

表 12-2-1 端口花费参考值

速 度	花费（修订后的 IEEE 规范）	花费（早先的 IEEE 规范）
10Gb/s	2	1
1Gb/s	4	1
100Mb/s	19	10
10Mb/s	100	100

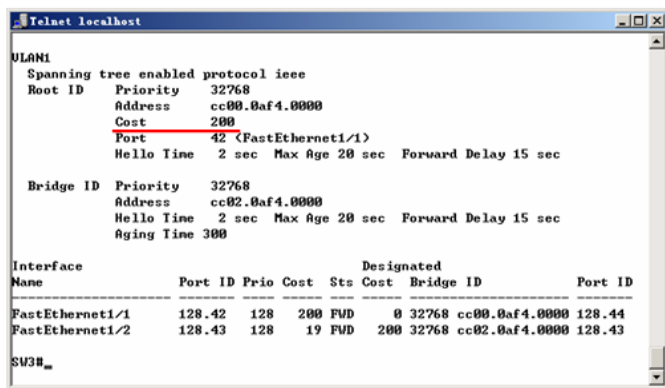
可以看出在早先的 IEEE（Institute of Electrical and Electronics Engineering，美国电气与电子工程师协会）标准中，是无法区分出千兆和万兆的。在修订后的 IEEE 规范中，100Mb/s 的链路花费是 19，可以从图 12-2-4 中得到验证，SW3 和 SW1 的花费是 19。

端口花费是可以修改的，重新运行 CCNA 机架中的 SW1 和 SW3，或者把 SW3 的优先级变回 32768。可以进行如下配置更改 SW3 的 Fa1/1 端口花费：

```
SW3(config)#int fa 1/1
SW3(config-if)#spanning-tree cost ?
<1-65535> Change an interface's spanning tree path cost
SW3(config-if)#spanning-tree cost 200
```

(2) **路径花费**。在图 12-2-4 中，已经看到 SW3 到 SW1 的路径花费是 19，前面修改了 SW3 的 Fa1/1 端口的花费为 200，接下来，再修改 SW1 的 Fa1/3 端口的花费为 2000。使用命令验证 SW3 到 SW1 的路径花费是 200 还是 2000，结果如图 12-2-6 所示。

在图 12-2-6 中，SW3 到 SW1 的花费是 200 而不是 2000，也就是前面提到的“从根交换机到达最终交换机前进方向上进入方向的端口花费”。如果经过多台交换机才到达根交换机，路径花费等于中间经过多条路径花费的总和。



```

Telnet localhost
SW3#
SW3#show spanning-tree
Spanning tree enabled protocol ieee
Root ID    Priority    32768
           Address    cc00.0af4.0000
           Cost        200
           Port        42 (FastEthernet1/1)
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID   Priority    32768
           Address    cc02.0af4.0000
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time  300

Interface   Port ID Prio Cost Sts Cost Bridge ID Port ID
-----
FastEthernet1/1  128.42  128  200 FWD  0 32768 cc00.0af4.0000 128.44
FastEthernet1/2  128.43  128   19 FWD  200 32768 cc02.0af4.0000 128.43
SW3#
  
```

图 12-2-6 修改路径花费

12.2.2 BPDU**

前一小节介绍了交换机间通过交换 BPDU 来选择根桥，本小节将介绍 BPDU 帧的细节。BPDU 帧包含 12 个字段，用来传输供 STP 使用的路径和优先级等信息。12 个字段的具体名称和所占的字节数，如图 12-2-7 所示。

这里对部分有用的字段进行解释。

- **Flags:** 标记域。包含了这些信息：TC（Topology Change，拓扑改变）比特位，表示拓扑发生改变事件；TCA（Topology Change Acknowledgment，拓扑改变确认）比特位，表示收到了拓扑变化通知，进行确认。
- **Root ID:** 根交换机的 BID。
- **Cost of path:** 到根交换机的路径花费。
- **Bridge ID:** 转发 BPDU 的交换机的 BID。
- **Port ID:** 转发 BPDU 的交换机的端口 PID，等于端口优先级（默认是 128）+端口编号。
- **Message age:** BPDU 已经存在的时间。
- **Max age:** BPDU 的最大存在时间。
- **Hellotime:** 根桥发送配置信息的间隔时间，这个值默认是 2 秒。
- **Forward delay:** 转发延迟。

Bytes	Field
2	Protocol ID
1	Version
1	Message type
1	Flags
8	Root ID
4	Cost of path
8	Bridge ID
2	Port ID
2	Message age
2	Max age
2	Hellotime
2	Forward delay

图 12-2-7 交换机的 BPDU

12.2.3 端口角色***

当 STA 决定使用哪一条路径之后，STA 配置交换机的端口角色，端口角色描述了它与根桥的关系和是否允许转发流量。交换机的端口角色有：

(1) **根端口（Root Port，简称 RP）。**非根交换机上离根交换机最近的端口称做根端口，每个非根交换机上有且仅有一个根端口。在图 12-2-1 中，SW1 是根交换机。SW2 从 Fa1/2 可以到达根交换机，花费是 19；从 Fa1/3 经 SW3 也可以到达根交换机，花费是 38（19+19=38）。相比之下，SW2 从 Fa1/2 到根交换机最近，所以 Fa1/2 是 SW2 的根端口。同理，SW3 的 Fa1/1 是 SW3 的根端口。

(2) **指派端口（Designated Port，简称 DP）。**每个网段都有一个指派端口，指派端口是该网段到根交换机最近的交换机上的端口。在图 12-2-1 中，SW1 上的 Fa1/1 和 Fa1/3 端口是指派端口，因为在 SW1 和 SW2 之间的网段上，SW1 本身就是根交换机，到根交换机的花费是 0，SW2 到根交换机的花费是 19，所以 SW1 上的 Fa1/1 是 SW1 和 SW2 之间网段上的指派端口；同理，SW1 上的 Fa1/3 是 SW1 和 SW3 之间网段上的指派端口。由此可以得出结论，在根交换机与非根交换机相连的网段上，根交换机上的端口都是指派端口。在 SW2 和 SW3 相连的网段上，两个非根交换机到根交换机 SW1 的花费都是 19，如何判断哪一个端口是指派端口呢？有关这个问题，将在“STP 收敛”一节专门讲解，这里先认为 SW2 上的 Fa1/3 端口是 SW2 和 SW3 之间网段上的指派端口。

(3) **非指派端口。**既不是根端口，也不是指派端口的激活端口称做非指派端口，在图 12-2-8 中，SW3 上的 Fa1/2 端口是非指派端口。非指派端口处在 Blocking（阻塞）状态，用来阻止环路。根端口和指派端口都在 Forwarding（转发）状态。

(4) **禁用端口。**被管理员使用“shutdown”命令关闭的端口称做禁用端口，禁用端口不参与生成树算法。在图 12-2-8 中，SW1 上的 Fa1/2 端口和 SW2 上的 Fa1/1 端口都是被禁用的端口。

12.2.4 端口状态和 BPDU 时间***

互连交换机间通过在一个广播域中交换 BPDU 帧构建一个逻辑上无环的路径。为了

使用这个逻辑生成树，交换机的端口需要在 5 种状态间转换，转换会经历 3 种 BPDU 时间。端口状态的转换和经历的时间，如图 12-2-9 所示。

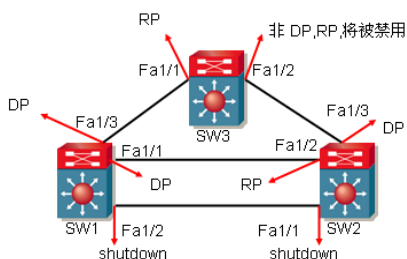


图 12-2-8 端口角色

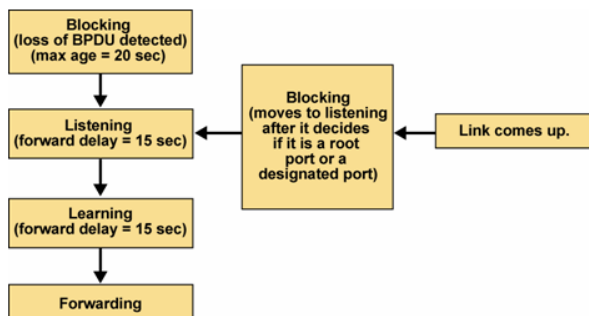


图 12-2-9 生成树的端口状态和 BPDU 时间

1. 端口状态转换

当交换机启动后，如果一个交换机端口直接转换到转发状态可能会形成暂时性的环路，这是由于交换机并不清楚整个网络的拓扑造成的，因为这个原因，STP 引入了 5 种端口状态：Down、Blocking、Listening、Learning、Forwarding。端口状态的改变过程如下：

① Down（禁用）状态。可以使用“no shut”命令和插入网线进行激活。

② Blocking（阻塞）状态。链路激活，端口转换到 Blocking 状态，这个状态会逗留大约 20 秒时间，主要用来决定该端口的角色，如果该端口是根端口或指派端口，将转换到下一状态；如果该端口是非指派端口，状态继续停留在 Blocking 状态；本来处在 Blocking 状态的端口，如果接收不到 BPDU 了，也会转换到下一状态。

③ Listening（侦听）状态。除了接收 BPDU 外，还向邻居交换机发送 BPDU，通知邻居交换机它将参与激活拓扑。这个状态会逗留大约 15 秒时间。

④ Learning（学习）状态。开始学习 MAC 地址。这个状态会逗留大约 15 秒时间。

⑤ Forwarding（转发）状态。端口可以转发数据帧。

2. 端口所处状态的功能

处在每种状态的端口都有什么功能对大家来讲是比较难于理解和记忆的，表 12-2-2 中对端口的状态（每一列）和功能（第一行）做了一个对比，其中“√”表示行头的端口具有列头的功能，其中“×”表示行头的端口不具有列头的功能。端口状态每前进一步就多一种功能，比如 Learning 状态可以接收 BPDU 帧、发送 BPDU 帧、学习 MAC 地址，但不能转发数据。

表 12-2-2 STP 端口状态功能表

	接收 BPDU	发送 BPDU	学习 MAC	转发 DATA
Down	×	×	×	×
Blocking	√	×	×	×
Listening	√	√	×	×
Learning	√	√	√	×
Forwarding	√	√	√	√

3. BPDU 的时间

BPDU 中相关的时间参数有：Hello time、Max age、Forward delay，可以通过图 12-2-10 中的命令进行修改，一般不建议修改 BPDU 的时间参数。

Hello 时间控制了发送配置 BPDU 的时间间隔，802.1D 标准规定其默认值为 2 秒。这个值实际上只控制配置 BPDU 在根网桥上生成的时间，其他网桥则把它们从根网桥收到的 BPDU 向外通告。如果在 2~20 秒内由于网络故障而没有收到新的 BPDU，非根网桥在这段时间内就停止发转发 BPDU。如果这种情况持续超过 20 秒，也就是超过默认的最大存活期，非根网桥就使原来储存的 BPDU 无效，并开始寻找新的根端口。所谓最大存活期，就是网桥在丢弃 BPDU 之前用来备份储存它的时间。

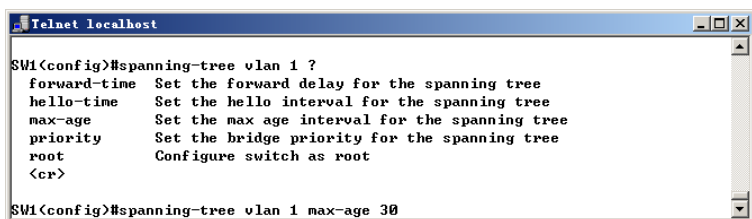


图 12-2-10 修改 BPDU 时间参数

转发延迟是网桥在侦听状态和学习状态所花费的时间，它的默认值是 15 秒。这个值是假定网络的最大规模为 7 段网桥相连、BPDU 的最大丢失个数为 3，以及 Hello 时间间隔为 2 秒的情况下得到的。

使用 STP 计时器的时候要注意，在没有仔细考虑之前，不要改变计时器的默认值。如果需要改变 STP 计时器的值，最好只在根桥上改变，这是因为根网桥的 BPDU 的 3 个字段中包含了计时器的数值，它可以把该计时器值从根网桥通告到网络中的其他网桥上。

12.3 STP 收敛***

收敛是生成树的一个重要方面。所谓收敛，就是整个网络达到一个稳定的状态，选举出根交换机，并决定出所有端口的角色，排除所有潜在的环路。当网络拓扑发生变化时，执行生成树算法，让网络重新收敛。

12.3.1 生成树的选举***

为了使采用 STP 的网络最终收敛为一个逻辑上没有环路的网络拓扑，需要通过以下 4 步实现。

- ① 每个广播域只能有一个根交换机。
- ② 每个非根交换机有且只有一个根端口。
- ③ 每个网段有且只有一个指派端口。
- ④ 既不是根端口，也不是指派端口的端口将被阻塞。

1. 选举根交换机

交换机之间通过发送 BPDU (Bridge Protocol Data Unit) 来选举根交换机，拥有最小 BID 的交换机将成为根交换机，有关根交换机的选举已经在“12.2.1 STP 算法”节中讲解过。

2. 选举根端口

每个非根交换机有且仅有一个根端口。非根交换机上的根端口是从非根交换机到根交换机的最低路径花费的端口。非根交换机可能会从多个端口接收到根交换机的 BPDUs，根端口的选举依照下面的顺序：

① 最低花费的端口成为根端口。有关根端口花费比较可以参照“12.2.3 端口角色”一节。

② 在花费相同的情况下，比较发送者的 BID。在图 12-3-1 中，交换机 SW4 从端口 1 和端口 2 都能收到根交换机 SW1 的 BPDUs，两边的花费相同，都是 38。接下来比较的就是发送者的 BID。假设 SW2 的 BID 是 32768+2222.2222.2222，SW3 的 BID 是 32768+3333.3333.3333，SW2 的 BID 小，则 SW4 的端口 1 成为根端口。

③ 在发送者 BID 相同的情况下，比较发送者的 PID (Port ID)。在图 12-3-2 中，SW1 是根交换机，SW2 的 Fa1/1 和 Fa1/2 到根交换机的花费相同，都是 19，发送者的 BID 也相同（都是交换机 SW1 的 BID）。接下来比较的是发送者的 PID。PID=端口优先级+端口号，端口优先级占用一个字节，默认是 128，端口号在同一个模块上是顺序增加的，起始端口号与交换机的型号以及该模块所在的插槽有关。可以通过下面的命令更改交换机端口的优先级：

```
SW2(config)#int fa 1/1
SW2(config-if)#spanning-tree port-priority ?
<0-255> Change an interface's spanning tree priority
SW2(config-if)#spanning-tree port-priority 10
```

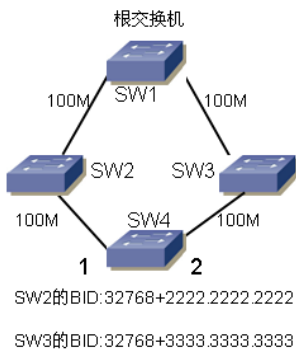


图 12-3-1 比较发送者的 BID

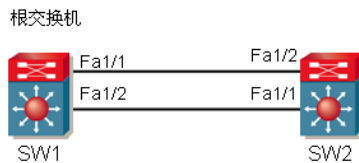


图 12-3-2 比较发送者的 PID

运行 CCNA 机架中的 SW1 和 SW2，然后在 SW2 上执行“show spanning-tree brief”命令，结果如图 12-3-3 所示。可以看到 SW2 交换机 Fa1/1 端口接收到的发送者 PID 是 128.43，Fa1/2 端口接收到的发送者 PID 是 128.42。SW2 的根端口是 Fa1/2 端口，根端口的状态是转发状态。

④ 在发送者 PID 相同的情况下，比较接收者的 PID。在图 12-3-4 中，SW1 是根交换机，SW1 的 Fa1/1 端口连接着 SW2 的 Fa1/1 和 Fa1/2，这样的拓扑往往是中间接了一台集线器。SW2 上两个端口的花费一样，发送者的 BID 也一样（都是 SW1 的 BID），发送者的 PID 也一样（都是交换机 SW1 的 Fa1/1 端口的 PID）。接下来将比较接收者的 PID。SW2 上 Fa1/1 端口的 PID 小于 Fa1/2 端口的 PID，SW2 的 Fa1/1 端口是根端口。

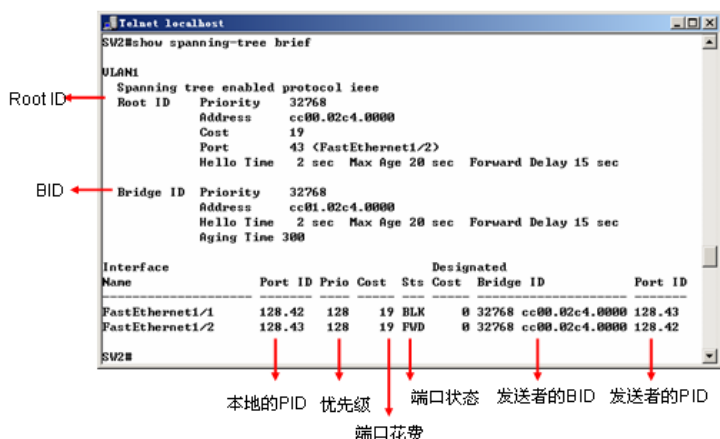


图 12-3-3 查看发送者的 PID

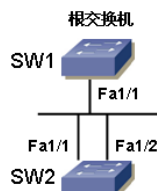


图 12-3-4 比较接收者的 PID

3. 选举指派端口

每个网段都有一个指派交换机，该交换机负责把网段的数据发往根交换机。指派交换机上的端口叫做指派端口。选举指派端口的过程其实是先选出指派交换机，如果指派交换机上有多个端口，再从多个端口中选出一个成为指派端口。指派端口的选举依照下面的顺序：

① **比较花费**。在图 12-3-5 中，SW1 是根交换机，SW2 到根交换机的花费是 4，SW3 到根交换机的花费是 8，在 SW2 和 SW3 之间的网段上，SW2 是指派交换机，则 SW2 上的 Gi2/3 端口是 SW2 和 SW3 之间的网段上指派端口。

② **比较 BID**。这里特别要提醒比较的是 BID，不是发送者的 BID，因为选举指派端口，首先要选出的是指派交换机，交换机的选举比较的则是 BID。在图 12-2-1 中，SW1 是根交换机，SW2 和 SW3 到根交换机的花费相同。接下来比较的是交换机的 BID，假如 SW2 的 BID 比 SW3 的 BID 小，则在 SW2 和 SW3 之间的网段上，SW2 是指派交换机，则 SW2 上的 Fa1/3 端口是 SW2 和 SW3 之间的网段上指派端口。

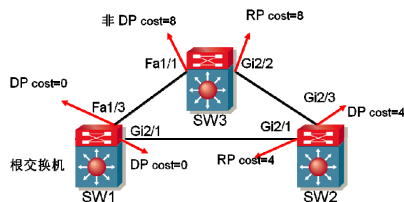


图 12-3-5 根据花费选举 DP

③ **比较 PID**。如果指派交换机上有多个端口连接到同一个网段，则具有最小 PID 的端口成为指派端口。

4. 阻塞端口

既不是根端口，也不是指派端口的端口将被阻塞。比如图 12-2-8 中 SW3 的 Fa1/2 端口、图 12-3-1 中 SW4 的端口 2、图 12-3-2 中 SW2 的 Fa1/2 端口、图 12-3-4 中 SW2 的 Fa1/2 端口、图 12-3-5 中 SW3 的 Fa1/1 端口都将被阻塞。

实验：正确配置 STP

运行 CCNA 机架中的 SW1、SW2 和 SW3，不做任何配置，分析各个端口的角色和状态。

① **选举根交换机**。在默认情况下，所有交换机的优先级都是 32768，SW1 的 MAC

地址 < SW2 的 MAC 地址 < SW3 的 MAC 地址。因此，SW1 的 MAC 地址最小，SW1 是根交换机。

② **选举根端口**。SW2 的 Fa1/2 和 SW3 的 Fa1/1 是根端口。

③ **选举指派端口**。SW1 上的 Fa1/1、Fa1/2、Fa1/3 和 SW2 上的 Fa1/3，这 4 个端口都是指派端口。

④ **阻塞端口**。SW2 上的 Fa1/1 和 SW3 上的 Fa1/2 既不是根端口，也不是指派端口，将被阻塞。

STP 收敛后的结果如图 12-3-6 所示，读者可以在每个交换机上使用“show spanning-tree brief”命令进行验证。

以下是笔者在工作中遇到的一个实例。

某单位网络拓扑如图 12-3-7 所示，在核心和汇聚层配置了两台思科 6509 交换机，两台交换机间使用千兆链路互连；接入层配置的是 2950 交换机，为了避免单链路故障，接入层使用两条百兆链路分别上连到两台 6509 交换机的 Fa2/1 端口；两台服务器均为千兆和思科 6509 交换机相连。公司员工反映网速很慢。经测试，发现两台服务器间的流量始终超过不了百兆。初步分析，可能是生成树的问题，在两台 6509 交换机上使用“show spanning-tree brief”命令查看，发现所有交换机的优先级都是默认的 32768，但 2950 生成的日期较早，有最小的 MAC 地址，交换机 2950 是根交换机。右边 6509 的 Gi1/1 端口既不是根端口，也不是指派端口，被阻塞。至此，原因找到了，由于 2950 是根交换机，两台 6509 间的千兆链路被阻塞，Server 1 到 Server 2 的流量全部经 2950 中转，百兆是瓶颈，这台 2950 交换机反而成了单位的核心。

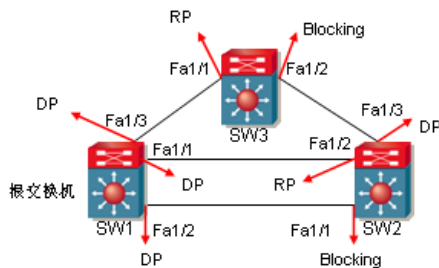


图 12-3-6 CCNA 机架中的默认生成树

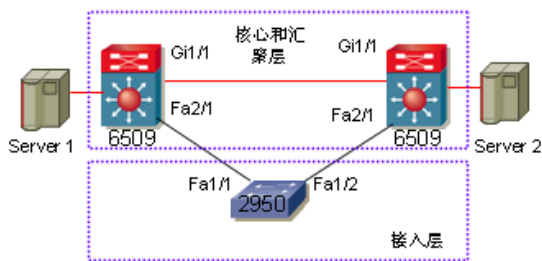


图 12-3-7 失败的 STP 配置

利用本章学到的知识，把两台 6509 交换机分别配置成根交换机和备份的根交换机，问题解决。

12.3.2 STP 拓扑变化**

当交换机检测到拓扑发生变化（交换机端口从转发状态变成阻塞状态；或者交换机端口变成转发状态，并且交换机上有一个指派端口）时，交换机通知根交换机拓扑变化了，根交换机再广播这个信息到整个网络中。

在正常的 STP 操作中，一个交换机从根端口接收根交换机发出的配置 BPDU，它从不向根交换机发送 BPDU。既然如此，它如何向根交换机通知拓扑变化信息呢？为了完成这个功能，一种特殊的 BPDU 被引入，叫 TCN（Topology Change Notification，拓扑改变通知）BPDU。当一个交换机需要通知拓扑改变时，该交换机开始从它的根端口向外发送 TCN

BPDUs，这种 TCN BPDU 是一种简化的 BPDU，不包含什么信息，在 Hello 间隔中发送。接收到这个 TCN BPDU 的交换机（这个网段的指派交换机），立即发回一个正常的 BPDU 进行确认，这个 BPDU 的 TCA（Topology Change Acknowledgement，拓扑改变确认）比特位被设置，该指定交换机产生一个 TCN BPDU。这样的过程重复下去，直至到达根交换机。

在图 12-3-8 中：

- ① S2 检测到拓扑变化，S2 从根端口向 D1 发送 TCN。
- ② D1 收到 S2 发过来的 TCN，D1 使用 TCA 向 S2 确认。
- ③ D1 产生 TCN，从根端口发给指派交换机 C1，也就是根交换机。
- ④ C1 收到 D1 发过来的 TCN，C1 使用 TCA 向 D1 确认。

一旦根交换机知道网络拓扑发生变化，它开始向外广播 TC（Topology Change）比特位被设置的配置 BPDU，如图 12-3-9 所示。这些 BPDU 被转发到网络中的所有交换机，最后，所有交换机都知道拓扑发生变化。根交换机发送 TC 比特位设置的配置 BPDU 的时间周期等于 Max age + Forward delay 秒，默认是 35 秒（20+15=35）。

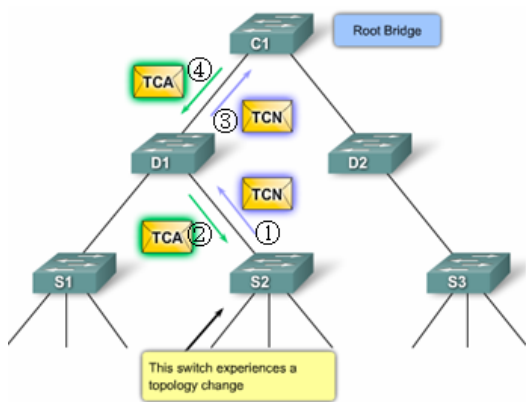


图 12-3-8 拓扑改变通知

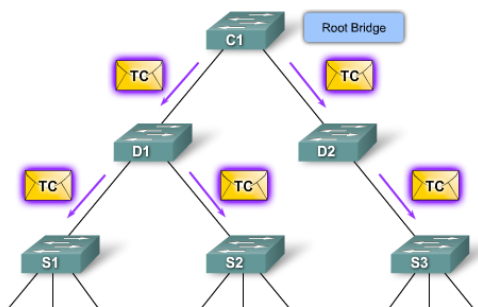


图 12-3-9 拓扑变化通知

12.3.3 增强的 STP 功能**

从前面的叙述中我们可以发现，启用 STP 功能的交换机，一个端口从 UP 到 Forwarding 大约需要 50 秒的时间；而普通的二层非网管型交换机，端口从 UP 到 Forwarding 瞬间就可以完成。单位领导可有意见了，便宜的交换机快，贵的交换机反而慢，钱花得不值呀！

如果只是从 VLAN 配置、STP、VTP 功能上讲，领导可能关心不了那么多细节问题，那来点直观的吧，用一根跳线，把普通的二层非网管型交换机连起来，让领导上网感受一下网络环路带来的问题，相信他会明白交换机支持 STP 的重要性。

其实启用 STP 功能的交换机经过合理配置，连接计算机的端口也能瞬间从 UP 到 Forwarding，办法就是把连接终端计算机的端口设成快速端口，实现的命令是：

```
SW1(config)#interface range fa1/1 - 10
SW1(config-if-range)#spanning-tree portfast
```

上面的命令把交换机的 Fa1/1 到 Fa1/10 共 10 个端口都设成快速端口，设置时，交换机控制台会提示，仅在连接计算机的端口上使用该功能，不要在连接集线器、交换机、网桥的端口上使用该功能，否则可能会导致临时性的生成树环路。同时还提示在 Trunk 端口使

用该功能是无效的。应该只在不会创建第 2 层环路的端口（例如连接 PC、服务器和路由器的端口）上使用 PortFast。



12.4 高级的 STP***

随着网络的发展，STP 产生了很多类型，它们有些是思科私有的，有些是 IEEE 标准。表 12-4-1 中描述了几种 STP 协议，本节仅介绍 PVST+和 RSTP。

表 12-4-1 思科和IEEE生成树协议对照表

思科私有	PVST (Per-VLAN STP, 每个 VLAN 一个生成树协议) 支持 ISL 封装协议 每个 VLAN 有一个生成树实例 能够实现第二层的负载均衡 支持 BackboneFast、UplinkFast 和 PortFast 特性
	PVST+ (Per-VLAN STP plus, 每个 VLAN 一个生成树协议加) 支持 ISL 和 802.1Q 封装协议 支持思科 STP 私有属性的扩展 增加了 BPDU guard 和 Root guard 功能
	Rapid-PVST+ (Rapid per-VLAN STP, 快速的每个 VLAN 一个生成树协议) 基于快速生成树的标准 比 802.1D 收敛的速度更快 支持 BackboneFast、UplinkFast 和 PortFast 特性
IEEE 标准	RSTP (Rapid STP, 快速生成树协议) 1982 年被提出, 比 802.1D 收敛的速度更快 实现思科普通私有属性的扩展 IEEE 把 RSTP 合成到 802.1D 中, 叫做 IEEE 802.1D—2004 规范
	MSTP (Multiple STP, 多生成树协议) 多个 VLAN 被映射到同一个生成树实例 IEEE 802.1Q—2003 现在包含 MSTP

12.4.1 PVST+**

最初的 802.1D 标准中，每个交换机仅支持一个生成树。思科发展 PVST 以使网络中的每个 VLAN 都有一个生成树（CCNA 机架中的模拟交换机仅支持 PVST+，并且不使用 Extended System ID）。然而，执行 PVST 意味着网络中的所有交换机参与生成树的收敛，交换机上的端口不得不提供更多的带宽来发送每一个 PVST+的生成树实例的 BPDU。

在 PVST+环境中，可以调整生成树参数使一半的 VLAN 走一条链路，另一半的 VLAN 走另一条链路。在图 12-4-1 中，网络中有两个 VLAN：VLAN 1 和 VLAN 2。在默认情况下，

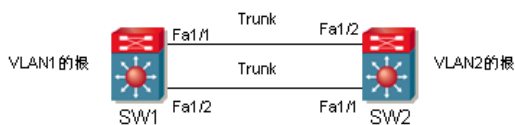


图 12-4-1 配置 PVST+

SW1 是 VLAN 1 和 VLAN 2 根交换机，针对 VLAN 1 和 VLAN 2，SW2 的 Fa1/1 端口都被阻塞，也就是说，SW1 和 SW2 之间所有的流量都从上面那条链路通过，下面这条链路不被使用。PVST 支持每个 VLAN 一个生成树，把

SW2 配置成 VLAN 2 的根, 针对 VLAN 2, SW1 的 Fa1/1 端口被阻塞, 也就是说, 针对 VLAN 2, 上面的链路被停用, 所有的流量都从下面的链路走。针对 VLAN 1 的流量仍然从上面走, 当两条链路中的任何一条链路故障时, 所有 VLAN 的流量都从剩下的那条链路走, 实现了两条链路的负载均衡和冗余备份。

SW1 的所有配置如下:

```
SW1#vlan data
SW1(vlan)#vlan 2
SW1(vlan)#exit
SW1#conf t
SW1(config)#int fa 1/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#int fa 1/2
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit
SW1(config)#spanning-tree vlan 1 root primary
```

SW2 的所有配置如下:

```
SW2#vlan data
SW2(vlan)#vlan 2
SW2(vlan)#exit
SW2#conf t
SW2(config)#int fa 1/1
SW2(config-if)#switchport mode trunk
SW2(config-if)#int fa 1/2
SW2(config-if)#switchport mode trunk
SW2(config-if)#exit
SW2(config)#spanning-tree vlan 2 root primary
```

配置完成后, 在 SW1 上验证结果, 如图 12-4-2 所示。

从图中可以看出针对 VLAN 1, SW1 的 BID 等于 Root ID, SW1 是 VLAN 1 的根交换机, 两个端口都是指派端口, 都处在转发状态; 针对 VLAN 2, SW1 的 BID 不等于 Root ID, SW1 不是 VLAN 2 的根交换机, Fa1/1 端口被阻塞。这样就实现了 VLAN 1 的流量从上面链路走, VLAN 2 的流量从下面链路走, 两条链路可负载均衡, 并起到冗余作用。

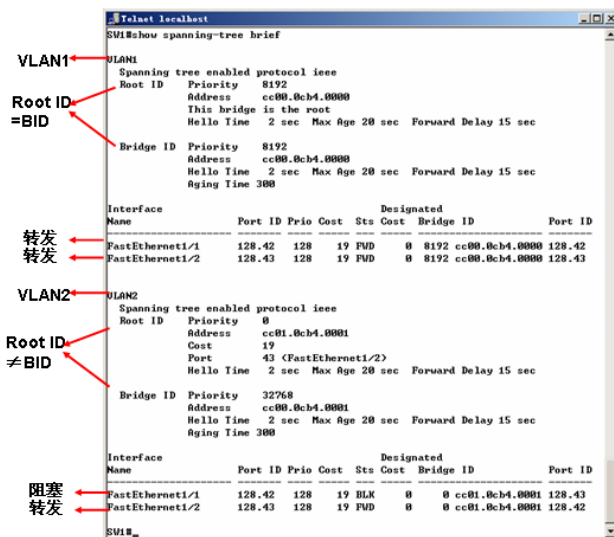


图 12-4-2 PVST 生成树

12.4.2 RSTP**

RSTP (IEEE 802.1w) 是从 STP (802.1D) 标准发展而来的。RSTP 的很多术语和 STP 相同, 大部分参数被保留下来, 因此熟悉 STP 协议的用户可以很快配置 RSTP。当第二层拓扑发生变化时, RSTP 加速了生成树的重新计算, 有时用不到 1 秒的时间就可完成收敛。RSTP 重新定义了端口的类型和状态。如果一个端口是替代端口或备份端口, 不需要等待网络的收敛立即就可以改变到转发状态。

思科 2960 交换机支持 PVST+、Rapid-PVST+ 和 MST, Packet Tracer 模拟器中的 2960 交换机支持 PVST 和 Rapid-PVST。可以使用下面的命令更改交换机 STP 的模式:

```
Cisco2960(config)#spanning-tree mode ?
mst          Multiple spanning tree mode
pvst         Per-Vlan spanning tree mode
rapid-pvst   Per-Vlan rapid spanning tree mode
Cisco2960(config)#spanning-tree mode rapid-pvst
```

在图 12-4-3 中, 显示了 RSTP 的端口角色、交换机 SW1 是根交换机, 有两个指派端口处在转发状态; SW2 上有一个根端口、一个指派端口、还有一个备份端口 (指派交换机上的非 DP 端口), 记住图 12-4-3 有助于区分备份端口和替代端口; SW3 上有一个根端口、一个替代端口 (非指派交换机上的端口)。

1. RSTP 的特点

- RSTP 是首选的阻止二层网络环路的协议。
- RSTP 不兼容 802.1D 的部分增强特性, 如 UplinkFast 和 BackboneFast 等。
- RSTP 向后兼容传统的 STP。
- RSTP 可以把一个端口安全地过渡到转发状态而不依赖于任何时间的配置。
- RSTP 保持和 STP 同样的 BPDU, 除了版本域和标记域有些不同外。
- RSTP 有很多增强, 比如在 BPDU 包中向邻居发送端口角色信息。

2. RSTP 的 BPDU

RSTP 使用版本 2 的 BPDU, RSTP 的标记 (flags) 字节和 STP 有稍许的不同。不像 STP, 任何 RSTP 的交换机即使没有从根交换机收到 BPDU, 每隔 Hello 时间 (默认 2 秒) 也会发送自己的 BPDU。所以 BPDU 也被用做保活 (keepalive) 检测, 连续丢失三个 BPDU 暗示着和邻居交换机的连接丢失, 这种机制能够快速检查到链路失败。

RSTP 更充分地利用了标记字节, 如图 12-4-4 所示, 在目前的 CCNA 考试中, 涉及标记字节的不多, CCNP 中会更深入地讨论标记字节。

- 与 STP 一样, 比特位 7 被用做拓扑变化通知, 比特位 0 被用做拓扑变化确认。
- 在快速收敛过程中, 比特位 6 被用做建议, 比特位 1 被用做同意。
- 比特位 2 和比特位 3 表示端口的状态: 丢弃、学习和转发。
- 比特位 4 和比特位 5 表示端口角色: 替换 (Alternate) 端口或备份 (Backup) 端口、根端口和指派端口。

3. 边缘端口

RSTP 的边缘端口是指交换机上从来不会连接到另一台交换设备的端口, 它可以被立即转换到转发状态。

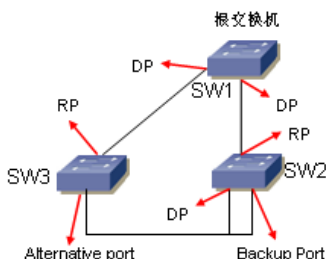


图 12-4-3 RSTP 的端口角色

RSTP Version 2 BPDU		Flag Field	
Field	Byte Length	Field	Bit Length
Protocol ID=0x0000	2	Topology Change	7
Protocol Version ID= 0x02	1	Proposal	6
BPDU Type= 0x02	1	Port Role	4-5
Flags	1	Unknown Port	00
Root ID	8	Alternate or Backup Port	01
Root Path Cost	4	Root Port	10
Bridge ID	8	Designated Port	11
Port ID	2	Learning	3
Message Age	2	Forwarding	2
Max Age	2	Agreement	1
Hello Time	2	Topology Change Acknowledgement	0
Forward Delay	2		

图 12-4-4 RSTP 的 BPDU

边缘端口和生成树中的 PortFast 一样，也是连接到最终的工作站，配置边缘端口的命令和配置 PortFast 端口的命令相同。当边缘端口禁用或启用时，不会产生拓扑改变。

边缘端口和 PortFast 端口也有区别，当 RSTP 的边缘端口收到 BPDU 时，该端口立即失去边缘端口的状态，变成一个正常的生成树端口。

4. 链路类型

在 RSTP 中，当某些端口的链路类型参数满足时，可以被快速地转换到转发状态。边缘端口被当做点对点链路，可以被直接过渡到转发状态；非边缘端口有两种链路类型：点到点链路类型和共享链路类型。链路类型可以被自动检测到，如果是全双工链路就是点到点链路，如果是半双工链路则是共享链路，也可以在交换机端口上明确规定端口的双工类型来确定链路的类型。

是否使用链路类型参数和端口的角色有关：

- 根端口不使用链路类型参数，根端口可以快速地转换到转发状态。
- 替换端口和备份端口在多数场合下也不使用链路类型参数。
- 使用链路类型参数最多的是指派端口，如果链路类型是点对点类型，指派端口可以快速地转换到转发状态。

5. 端口角色和端口状态

RSTP 的端口状态有 3 种：丢弃（Discarding）、学习（Learning）和转发（Forwarding）。RSTP 的端口状态和 STP 的端口状态对应如表 12-4-2 所示。

表 12-4-2 RSTP和STP端口状态对照表

STP 端口状态	RSTP 端口状态
Disable	Discarding
Blocking	Discarding
Listening	Discarding
Learning	Learning
Forwarding	Forwarding

RSTP 的端口角色有 5 种：

- 根端口：同 STP 的根端口，转发数据。

- **指派端口**：同 STP 的指派端口，转发数据。
- **替换端口**：到根网桥的替换路径，用以替换当前的根端口。替换端口在生成树拓扑稳定的情况下，处于丢弃状态。
- **备份端口**：由指定端口提供的到生成树叶结点的备份路径。备份端口只存在于这两种情况下：两端口通过点到点链路相连成一个环路；网桥与共享 LAN 网段有两条或两条以上的连接，如图 12-4-3 所示。备份端口在生成树拓扑稳定的情况下，处于丢弃状态。
- **禁止端口**：在生成树中不起作用的端口。

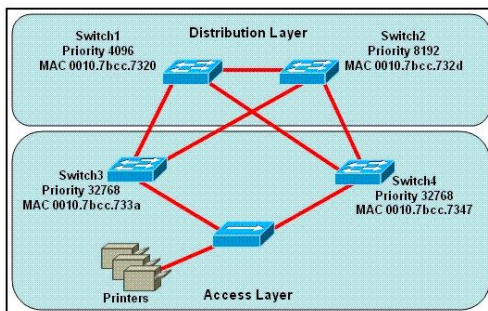


12.5 真题精选***

1. Which two values are used by Spanning Tree Protocol to elect a root bridge? (Choose two.)

- A. amount of RAM B. bridge priority C. IOS version
D. IP address E. MAC address F. speed of the links

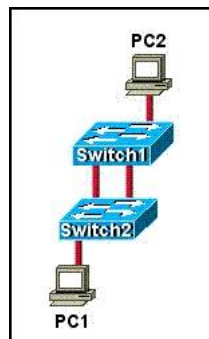
2. Refer to the exhibit. Which switch provides the spanning-tree designated port role for the network segment that services the printers?



- A. Switch1 B. Switch2
C. Switch3 D. Switch4

3. Refer to the exhibit. When PC1 sends an ARP request for the MAC address of PC2, network performance slows dramatically, and the switches detect an unusually high number of broadcast frames. What is the most likely cause of this?

- A. The portfast feature is not enabled on all switch ports.
B. The PCs are in two different VLANs.
C. Spanning Tree Protocol is not running on the switches.
D. PC2 is down and is not able to respond to the request.
E. The VTP versions running on the two switches do not match.



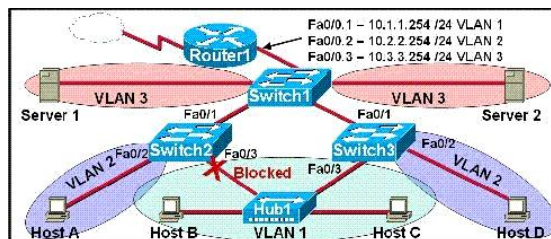
4. In which circumstance are multiple copies of the same unicast frame likely to be transmitted in a switched LAN?

- A. during high traffic periods
B. after broken links are re-established

- C. when upper-layer protocols require high reliability
 D. in an improperly implemented redundant topology
 E. when a dual ring topology is in use
5. A network administrator needs to force a high-performance switch that is located in the MDF to become the root bridge for a redundant path switched network. What can be done to ensure that this switch assumes the role as root bridge?
- A. Establish a direct link from the switch to all other switches in the network.
 B. Assign the switch a higher MAC address than the other switches in the network have.
 C. Configure the switch so that it has a lower priority than other switches in the network.
 D. Configure the switch for full-duplex operation and configure the other switches for half-duplex operation.
 E. Connect the switch directly to the MDF router, which will force the switch to assume the role of root bridge.
6. Refer to the exhibit. The output that is shown is generated at a switch. Which three of these statements are true? (Choose three.)

```
Switch# show spanning-tree vlan 30
VLAN0030
Spanning tree enabled protocol rstp
Root ID Priority 24606
Address 00d0.047b.2800
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 24606 (priority 24576 sys-id-ext 30)
Address 00d0.047b.2800
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface Role Sts Cost Prio.Nbr Type
-----
Fa1/1 Desg FWD 4 128.1 p2p
Fa1/2 Desg FWD 4 128.2 p2p
Fa5/1 Desg FWD 4 128.257 p2p
```

- A. All ports will be in a state of discarding, learning, or forwarding.
 B. Thirty VLANs have been configured on this switch.
 C. The bridge priority is lower than the default value for spanning tree.
 D. All interfaces that are shown are on shared media.
 E. All designated ports are in a forwarding state.
 F. This switch must be the root bridge for all VLANs on this switch.
 7. Which statement is correct about the internetwork shown in the diagram?

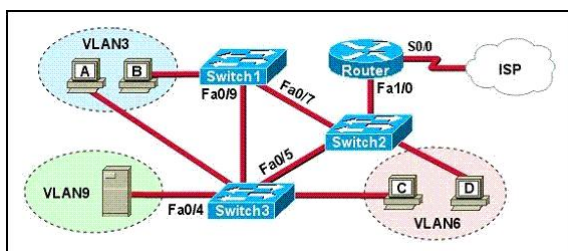


- A. Switch 2 is the root bridge.
 B. Spanning Tree is not running.
 C. Host D and Server 1 are in the same network.

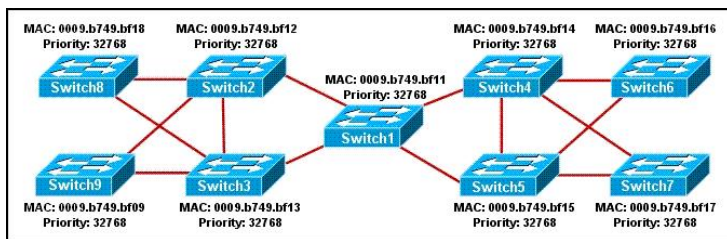
- D. No collisions can occur in traffic between Host B and Host C.
- E. If Fa0/0 is down on Router 1, Host A cannot access Server 1.
- F. If Fa0/1 is down on Switch 3, Host C cannot access Server 2.

8. Refer to the exhibit. A problem with network connectivity has been observed. It is suspected that the cable connected to switch port Fa0/9 on Switch1 is disconnected. What would be an effect of this cable being disconnected?

- A. Host B would not be able to access the server in VLAN9 until the cable is reconnected.
- B. Communication between VLAN3 and the other VLANs would be disabled.
- C. The transfer of files from Host B to the server in VLAN9 would be significantly slower.
- D. For less than a minute, Host B would not be able to access the server in VLAN9. Then normal network function would resume.



9. Refer to the exhibit. The switches on a campus network have been interconnected as shown. All of the switches are running Spanning Tree Protocol with its default settings. Unusual traffic patterns are observed and it is discovered that Switch9 is the root bridge. Which change will ensure that Switch1 will be selected as the root bridge instead of Switch9?



- A. Lower the bridge priority on Switch1.
- B. Raise the bridge priority on Switch1.
- C. Lower the bridge priority on Switch9.
- D. Raise the bridge priority on Switch9.
- E. Disable spanning tree on Switch9.
- F. Physically replace Switch9 with Switch1 in the topology.



12.6 真题解答***

1. 解: BE

题目问: 哪两个值被用来选举生成树的根桥? 首先, 要知道生成树根桥的选举是比较

交换机的 BID，谁的 BID 最小，谁就是根交换机；其次，要知道 BID 的由来，BID 主要由 3 部分组成：优先级+Extended System ID（可选）+交换机的 MAC 地址。在不使用 Extended System ID 的情况下，只需比较桥优先级和 MAC 地址；在使用 Extended System ID 的情况下，因为 Extended System ID 和 VLAN 号相同，所有同一个广播域中参与选举根桥的交换机的 Extended System ID 是相同的。结论是：不管是否使用 Extended System ID，根桥的选举只需要比较桥优先级和 MAC 地址。具体请参阅本章 12.2.1 小节的内容。

2. 解：C

题目问：打印机所在的这个网段（冲突域），哪一个端口是指派端口？第一步，需要找到根桥，而根桥的选举是通过比较 BID 实现的，而且是越小越优先，BID 的组成为桥优先级和 MAC 地址。所以我们通过图可以找到根桥为 Switch1。第二步，在非根桥上选出根端口，通过比较到根桥的花费来选举的，花费最小的就是根端口。图中没有表示出链路的带宽，则只能假想所有链路的带宽相同（笔者估计摘录有误，考题中应该有带宽说明）。第三步，选举指派端口。每条链路都需要有一个 DP，选 DP 其实是选每个网段的指派交换机，因为 Switch3 和 Switch4 到根的花费一样，接下来比的就是 BID，Switch3 有更小的 BID，Switch3 是打印机所在网段的指派交换机，Switch3 上的端口是指派端口。具体请参阅本章 12.3.1 小节的内容。

3. 解：C

题目问：当 PC1 发出一个 ARP request 查询 PC2 的 MAC 地址时，网络性能下降严重，交换机检测到有大量的广播帧存在，最可能是什么原因造成这个现象的？首先，要清楚 ARP request 是以广播的形式发送出去的。当 ARP 报文传到 Switch2 时，交换机对广播的流量是以泛洪的形式处理的，报文就从除了连接 PC1 的端口外的所有端口都发出去了。Switch1 收到广播后也泛洪，因此一个广播环路就产生了，网络性能变得很差，因为广播的流量占有了很大的带宽。而我们阻断二层环路是通过运行生成树协议来实现的，在图中有环路存在，说明没有运行生成树协议。具体请参阅本章 12.1 节的内容。

4. 解：D

题目问：在交换机互连的局域网中，在什么环境下一个单播帧会出现多个拷贝？本章讲到冗余拓扑会带来 3 个问题：广播风暴、MAC 地址的不稳定、重复的单播帧的拷贝。具体请参阅本章 12.1 节的内容。

5. 解：C

题目问：一个网络管理员想强制让 MDF（总配置线架）中的一台高性能交换机成为冗余拓扑中的根桥，什么做法能确保这台交换机成为根交换机？根桥的选举是通过比较 BID 来实现的，而 BID 由桥优先级和 MAC 地址组成，越小越优先。因此想让哪台交换机成为根桥，把它的优先级配置得比其他交换机的都低就可以了。

6. 解：ACE

这个题有一定的难度。题目问：从图中的输出，可以得出哪三个选项是正确的？本章 12.4.2 小节中提到 Cisco 2960 交换机上仅支持 PVST+、Rapid-PVST+ 和 MSTP 三种生成树协议。在思科交换机上，“show spanning-tree”的时候，如果配置的是 PVST+，显示使用的

生成树协议是“ieee”；如果配置的是 Rapid-PVST+，显示使用的生成树协议是“rstp”；如果配置的是 MSTP，显示使用的生成树协议是“mst”。从图中的输出可以看出，交换机执行的是 Rapid-PVST+，RSTP 的端口状态有三种，A 选项是正确的。B 选项说交换机上配置了三个 VLAN，从图中的输出得不到这个结论。从图中可以看出，这台交换机的优先级是 24576，如果考虑到 Extended System ID，则优先级是 24606，不管哪一个，都低于交换机的默认优先级 32768，所以 C 选项是正确的。从图中的输出可以看出，所有的端口类型都是 p2p（点到点），并不是共享链路，所以 D 选项是错误的。从图中的输出可以看出，所有的端口角色都是指派端口，状态都是转发状态，所以 E 选项是正确的。Rapid-PVST+ 是每个 VLAN 的一个生成树实例，想想本章的图 12-4-1 中，一台交换机可以是一个 VLAN 的根，另一台交换机可以成为另一个 VLAN 的根，从图中仅能得出这台交换机是 VLAN 30 的根桥，所以 F 选项是错误的。

7. 解：E

这个题有一定的难度。题目问：从图中可以得出哪个结论是正确的？本题涉及多个交换机以及多个 VLAN 间的通信。而在交换机之间有一个环路，因此生成树阻断了其中的一个端口，所以运行了生成树协议，B 选项错。根据生成树的原理，Blocked 的端口是在非根桥上的，因此 Switch 2 不会是根桥，所以 A 选项错。而 Host D 和 Server 1 一看就不在相同的 VLAN 内，因此是在不相同的网络中的，所以 C 选项错。我们说整个 Hub 是一个大的冲突域和广播域，而 Host B 和 Host C 接在同一台 Hub 上，它们之间是有冲突存在的，所以 D 选项错。Host A 和 Server 1 在不同的 VLAN 之间，它们之间通信是要借助于 Router 1 的端口 Fa0/0 的子端口来实现的，如果 Router 1 的 Fa0/0 端口 Down 了，那么 Host A 和 Server 1 之间就无法通信了，所以 E 选项正确。如果 Switch 3 的 Fa0/1 端口 Down 了，那么生成树就会重新选举，以前 Blocked 的端口就会开始转发数据，Host C 就通过 Switch 2 将它的数据发送出去，它仍然可以访问 Server 2，所以 F 选项错。

8. 解：D

题目说：怀疑 Switch 1 的 Fa0/9 有问题，如果 Switch 1 的 Fa0/9 连线断开，会有什么影响？三台交换机间有一个环路存在，断开三台交换机间的任何一条链路，都会引起拓扑的变化，生成树需要重新收敛，STP 生成树的收敛过程 1 分钟之内即可完成。在生成树的收敛过程中，交换机是不转发数据包的。当生成树收敛完成后，整个网络通信恢复正常。综上所述，只有 D 的说法正确，Host B 小于 1 分钟的时间不能访问 VLAN 9 中的服务器，然后正常的网络功能恢复。

9. 解：A

题目问：参照图，园区网络中的交换机被互连，所有的交换机都使用默认值启用了生成树协议。Switch 9 被发现是根交换机，造成流量很不合理。做什么改变可以确保 Switch 1 能够代替 Switch 9 成为根交换机？观察图中所有交换机的优先级都是 32768，Switch 1 的 MAC 地址只比 Switch 9 大。应该说这题出得不严谨，降低 Switch 1 的优先级（A 选项）、升高 Switch 9 的优先级（D 选项）或禁用 Switch 9 的生成树协议（E 选项），都可以使 Switch 1 成为根交换机，可是如果园区网络中又新增了一台有默认配置的交换机，难保 MAC 地址不比 Switch 1 的 MAC 地址小，Switch 1 并不能稳定地成为根，最好的办法还是降低 Switch 1 的优先级。故 A 最正确。

第 13 章

无线网络***

本章主要介绍当前可使用的不同无线标准，以及每种标准的特点，无线网络中需要使用的硬件，部署和设计无线网络，无线网络相关的安全协议及特点，如何加强无线网络的安全，配置和排错无线网络。本章是 CCNA 640-802 考试新增加的内容，知识点不多，但在考试中所占的比重不少，读者需要认真阅读本章。



13.1 无线网络介绍**

有线网络有时是很局限的。想象一下，可以在办公室的任何位置随意放置电脑，可以在会议室用笔记本电脑进行演示，可以在篮球场或树荫下进行网上冲浪。如果是有线的网络就需要根据用户办公的位置调整布线，需要在会议室布线，需要在篮球场和室外进行布线，为了解决频繁变更布线和布线困难的问题，可以考虑使用无线，现在无线网络变得越来越流行。

13.1.1 使用无线网络*

网络改变了人们的生活和学习方式，在许多家庭，互联网和电视、电话一样，已成为一个标准的服务。为了使用方便，像固定电话扩展到移动电话一样，无线网络成为有线网络的扩展。

1. 无线网络的分类

无线网络根据连接范围有 PAN（Personal Area Network，个人网）、LAN（Local Area Network，局域网）、MAN（Metropolitan Area Network，城域网）和 WAN（Wide Area Network，广域网）之分，表 13-1-1 列出了这几种无线网络使用的标准、传输的速度、有效的范围和典型的应用。在一些企业和家中，无线最典型的应用就是无线局域网（Wireless Local Area Network，WLAN）。

表 13-1-1 无线网络的划分

	PAN	LAN	MAN	WAN
Standards（标准）	Bluetooth	802.11a、802.11b、802.11g	802.16 MMDS、LMDS	GSM、GPRS、 CDMA、2.5~3G
Speed（速度）	<1Mb/s	1~54Mb/s	22Mb/s	10~384kb/s
Range（范围）	Short（短）	Medium（中等）	Medium-long（中等偏长）	Long（长）

续表

	PAN	LAN	MAN	WAN
Applications (应用)	peer to peer、 device to device (端到端)、 设备到设备	Enterprise networks (企业 网络)	Fixed, last- mile access (固定的, 最 后 1 英里接入)	PDA (Personal Digital Assistant, 个 人数字助理)、 Mobile Phones (移 动电话)

2. 无线网络的好处

使用无线局域网，一个重要的好处是方便。用户可以不必局限在固定的位置，比如办公桌甚至办公室，也可以使用网络，如图 13-1-1 所示，无线网络可以作为有线网络的扩展，带来灵活和方便。

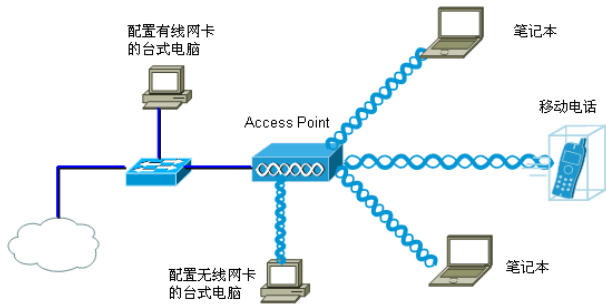


图 13-1-1 扩展有线网络线路

使用无线局域网，另一个好处是可以降低成本。举例来说，搬入一个临时性的办公场所，据统计，如果是采用有线，平均每个节点的费用是 375 美元。在这种情况下，使用无线局域网优势更明显，可以节省电缆通过墙壁、天花板、地板的花费。虽然难以衡量，但无线局域网可以产生更好的生产力和更宽松的工作环境，从而导致更好的结果，为企业增加利润。

3. 无线网络和有线网络的区别

WLAN 和以太网一样，都采用了 IEEE 的 802 标准。两个主导的 802 标准是 802.3 以太网和 802.11 无线局域网，二者之间有一些重要的不同。无线局域网和有线局域网的区别如表 13-1-2 所示。

表 13-1-2 无线局域网和有线局域网的区别

特 点	802.11 无线网	802.3 以太网
物理层	Radio Frequency (RF, 无线电频率)	Cable (线缆)
媒体访问的方式	Collision Avoidance (冲突避免)	Collision Detection (冲突检查)
可用性	在 AP 范围内的任何无线网卡	有线缆连接
信号干扰	易受干扰	不受干扰
规定	本地政府的额外规定	IEEE 标准规定

无线局域网使用的是无线电频率 (Radio Frequency, RF) 而不是电缆，和电缆相比，无线电频率有以下特点：易受干扰，包括吸收（墙壁，天花板和地板等都会吸收无线电波）、散射（粗糙的物体表面会无线电波散开）、反射（金属和玻璃会造成反射）；无线电频率没

有边界，缺乏这种边界，数据帧向任何能够接收无线电频率信号的地方发送，处在无线电频率范围内的无线网卡都可以接收到信号；在同一个地理区域，使用相同或类似的无线电频率可以互相干扰；在不同的国家，对无线电频率的使用有不同的规定。

无线局域网的客户端通过无线接入点（Access Point）连接到网络，而不是一个以太网交换机。无线网是一个共享网，一个 AP 就像以太网中的 Hub，数据在无线电波上传输，相同的无线电频率被用来发送和接收，网络中的设备越多，每个设备的吞吐量就越低。无线网络虽然可以实现双向通信，但只能采用半双工的方式，就像 Hub 一样，工作在半双工的模式下，收和发是不能同时进行的，除非接收和发送使用了不同的无线电频率。无线网络不同于有线网络，线缆上可以检测到有冲突信号，在无线的情况下，只要数据发送出去，就没有办法检测到是否有冲突发生，所以 802.11 采用的是“CSMA/CA”，采用的是 CA（Collision Avoidance，冲突避免）技术，而不是 CD（冲突检测）技术。

无线局域网需要更多地考虑安全问题，因为无线电频率可以到达任何有效的范围，很容易造成信息的泄密。

13.1.2 无线局域网标准***

802.11 无线局域网是一个 IEEE 标准，定义使用不需要许可的工业、科学和医疗（Industrial, Scientific, Medical，简称 ISM）频段的无线电频率如何被用于无线链路物理层和 MAC 子层。

当 802.11 首次发布时，规定了在 2.4GHz（赫兹是频率单位，频率用于测量波和交流电在 1 秒钟内的状态变化数或周期数，可以通过空气发送和接收各种波）频段进行 1~2Mb/s 的数据传输速率。当时，有线局域网上的运行速率是 10Mb/s，所以这个新的无线技术并没有被大量应用。自那时开始，无线局域网标准的不断发展提高，相继推出了 IEEE 802.11a、IEEE 802.11b、IEEE 802.11g、802.11n 的标准草案等。

在通常情况下，选择使用无线局域网标准是基于数据传输速率的。举例来说，802.11a 和 802.11g 可支持最快 54Mb/s，而 802.11b 最快支持 11Mb/s，因为 802.11b 标准速度比较慢，802.11a 和 802.11g 更受欢迎。第四版的 WLAN 草案提出了 802.11n 标准，802.11n 超过现有标准的数据传输速率，该标准于 2008 年 9 月被批准。

不同的无线局域网标准的数据速率受一些调制技术的影响。本节涉及两种调制技术：直接序列展频技术（Direct Sequence Spread Spectrum，DSSS）和正交频分复用（Orthogonal Frequency Division Multiplexing，OFDM）。读者不需要知道这些技术如何工作，但应该知道，当一个标准使用 OFDM 技术时，将会有更快的数据传输速率。DSSS 技术比 OFDM 简单，相对花费较少。

1. 802.11a

IEEE 802.11a 采用 OFDM 调制技术，并使用 5GHz 频段。802.11a 的设备使用 5GHz 的频段，不太容易受到用户家用设备的干扰，因为多数用户家用设备都使用 2.4GHz 频段，很少有使用 5GHz 频段的。此外，更高的频率允许使用较小的天线。

使用 5GHz 频段有一些重大的缺点。第一是较高频率的无线电波更容易被障碍物（比如墙）吸收，802.11a 易受障碍物的影响，而使性能变得很糟糕。第二是这种更高的频宽的有效范围比 802.11b 或 802.11g 略差。此外，一些国家包括俄罗斯，不容许使用 5GHz 频段，这可能影响其部署。

2. 802.11b 和 802.11g

802.11b 标准指定在 2.4GHz 频段使用 DSSS 调制技术，数据传输速率可以是 1、2、5.5 和 11Mb/s。

802.11g 在这一频段通过使用 OFDM 调制技术可以实现更高的数据传输速率。IEEE 802.11g 标准还规定，可以使用 DSSS 调制技术，向后兼容 IEEE 802.11b 标准。使用 DSSS 技术的速度是 1、2、5.5 和 11Mb/s，使用 OFDM 技术的数据传输速率是 6、9、12、18、24、48 和 54Mb/s。

使用 2.4GHz 频段也有优势。设备使用 2.4GHz 频段将比使用 5GHz 频段有更远的传输范围。此外，2.4GHz 频段的传输与 802.11a 工作在 5GHz 传输相比，不容易被阻碍。

使用 2.4GHz 频段有一个非常严重的缺点，许多消费性的电子设备也使用了 2.4GHz 频段，比如 baby monitors（婴儿监视器）、cordless phones（无绳电话）和 microwave ovens（微波炉），都会导致使用 802.11b 和 802.11g 的设备易受干扰。

3. 802.11n

IEEE 802.11n 标准草案的用意是改善无线局域网的数据传输速率和范围，而不需要额外的电源或无线电频段分配。802.11n 标准使用多个无线电频率和天线，在端点每个广播点用一个频率，多个频率可以建立多个流。这种多输入/多输出（MIMO）技术把一个高速率的数据流分成多个慢速率的数据流，在多个可用的频率和天线上把多个数据流同时广播出去。使用 2×2 天线的 802.11n 理论上数据速率最高可达 248Mb/s。

重要说明：RF 频段由国际电讯联盟的无线电通信部门（ITU-R）分配。该 ITU-R 指定 900MHz、2.4GHz 和 5GHz 频段用于 ISM 通信无须许可。虽然 ISM 频段在全球范围内无须许可，但它们仍然受到地方性法规的限制。

4. 几种无线局域网标准的对比

表 13-1-3 对几种标准做了对比，虽然难以记忆，但 CCNA 考试中经常涉及。

表 13-1-3 无线局域网标准对比

	802.11a	802.11b	802.11g	802.11n
频段	5GHz	2.4GHz	2.4GHz	2.4GHz 或 5GHz
没有重叠的通道	最多 23	3	3	14
IEEE 批准时间	1999 年 10 月	1999 年 10 月	2003 年 6 月	2008 年 9 月
数据速率	最快 54Mb/s	最快 11Mb/s	DSSS 最快到 11Mb/s; OFDM 最快到 54Mb/s	使用两个 MIMO 流， 248Mb/s（使用 2×2 天线），最新的说法理论 可达 600Mb/s
调制技术	OFDM	DSSS	OFDM DSSS	MIMO-OFDM
优点	速度快，不易受干扰	低花费，远的距离	快，远的距离，不易 被吸收	好的速率，远的距离
缺点	高花费，短的距离	慢，易受干扰，主要是 因为很多家电工作在 2.4GHz	易受干扰	不同厂商设备可能 不兼容

5. 与无线相关的三个组织

- ITU-R, 管理无线电频率频段的分配。
- IEEE, 指定无线电频率怎样被调制来传输信息。
- Wi-Fi, 确保不同厂商的设备可以协同工作。

13.1.3 无线局域网的组件*

大家可能已经在使用无线网络了, 在家里、咖啡馆里或在工作场所等地方。以无线方式接入本地网络或互联网需要什么样的硬件呢? 本节将介绍这些组件, 包括:

1. 无线网卡

无线局域网的组成是用户端连接到接入点, 用户端使用的是无线网卡, 无线网卡使客户工作站能够发送和接收无线电频率信号。无线网卡像一个以太网卡, 如图 13-1-2 所示, 使用调制技术, 把数据流编码后放到 RF 信号上。无线网卡经常与移动设备相连, 如笔记本电脑。



图 13-1-2 无线网卡

2. 无线 AP

一个 AP (Access Point, 接入点) 连接无线客户端到有线网络, 通常客户端设备不会直接通信, 它们通过 AP 通信。在本质上, 一个 AP 转换空气中 802.11 封装的帧格式到有线以太网上的 802.3 以太网帧格式。在无线网络中, 客户端必须连接到 AP 以获得网络服务, 连接就是客户端加入 802.11 网络的过程, 类似于连线到一个有线网络, 稍后讨论如何建立连接。

AP 的功能类似于 802.3 以太网中的 Hub, RF 是一个共享的媒体, AP 监听所有的无线电通信。无线电设备不能检测到冲突, 但无线设备可以设计使用 CSMA/CA 技术来避免冲突。

802.11 的 MAC 层采用的是 CSMA/CA (Carrier Sense Multiple Access /Collision Avoidance) 的冲突避免方法。CSMA/CA 要求每一个发送结点在发送帧之前需要先侦听信道, 如果信道空闲, 结点可以发送帧。发送站在发送完一帧之后, 必须再等待一个短的时间间隔, 检查接收站是否发回帧的确认 ACK。如果接收到确认, 则说明此次发送没有出现冲突, 发送成功; 如果在规定的时间内没有接收到确认, 表明出现冲突, 发送失败, 重发该帧, 直到在规定的最大重发次数之内, 发送成功。

在 CSMA/CA 中, 发送结点在发送帧之前要侦听信道, 如果信道空闲开始发送, 有时也会产生冲突。如图 13-1-3 所示, PC1 和 PC2 都可以到达 AP, 但在 AP 相反的方向上, 且与 AP 之间的距离很远, PC1 和 PC2 之间距离太远, 相互间不可到达, 彼此感受不到对方的存在, 它们可能会同时传递, 这就是所谓的隐藏结点问题。CSMA/CA 的 RTS/CTS (Request To Send/Clear To Send, 要求发送/发送完毕) 特性可以用来解决这种隐藏结点的问题。

RTS/CTS 被设计成允许客户端和 AP 之间进行协商。当在一个网络启用 RTS/CTS 后,设备准备传输数据时,先侦听无线电频率,确定目前是否正在传输信号,如果没有,此设备生成 RTS 信号,说明它有数据要发,AP 分配媒介(也就是无线电传输频率)给该设备足够长时间来完成所需的传送。当传输完成后,该设备发送一个 CTS 信号,表明其他无线设备现在可传输数据了。其他工作站以类似的方式向 AP 申请媒介,这样一般的冲突就被避免了。

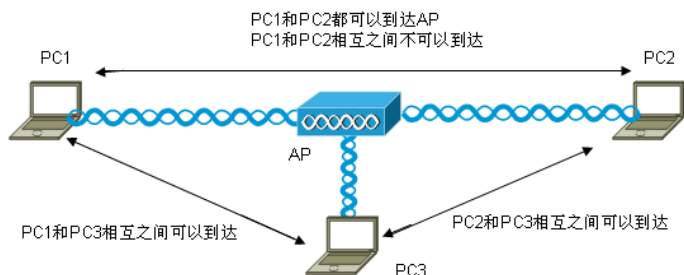


图 13-1-3 隐藏结点的问题

3. 无线路由器

无线路由器执行接入点、以太网交换机、路由器的角色。举例来说,Linksys WRT300N 是一个小公司或住宅最常用的无线接入设备,在预计负荷不是很大的情况下使用。在一个盒子中集成了三个功能,首先是一个无线接入点,可以执行典型的接入点功能;其次是一台交换机,内置了 4 个全双工 10/100Mb/s 端口,可以用来连接到有线设备;最后是一台路由器,提供了一个外网接口,用来连接其他网络设备,还可以对连接在 4 个交换端口以及无线接入的 PC 提供网关功能,实现共享上网。

13.1.4 实施无线***

1. 配置 AP 参数

建立客户端和 AP 的连接前,需要先配置 AP 的一些参数,包括:

(1) 模式

无线网络的模式是指 WLAN 协议: 802.11a、802.11b、802.11g 或 802.11n。因为 802.11g 向后兼容 802.11b,默认的无线网络模式是“混合”,如图 13-1-4 所示,混合意味着 AP 同时支持 802.11b 和 802.11g 标准。用户也可选择单一模式,比如 802.11b 或 802.11g。在混合模式下,如果所有连接到 AP 的客户端都是 802.11g 的,则所有的客户端工作在快速模式。当既有 802.11b 的客户端,又有 802.11g 快速客户端时,它们竞争通道,快速的客户端在发送数据之前需要等待 802.11b 的客户端清除通道。

(2) SSID

服务设置标识符(Service Set Identifier, SSID)是一个独特的标识符,也称无线网络名称,客户端设备使用 SSID 区分在同一地区的多个无线网络。在一个网络上的几个 AP 可以共用一个 SSID,这主要用在支持用户漫游的情况下。在图 13-1-4 中,显示该无线网络名称(SSID)是“linksys”,SSID 可以是任何字母(区分大小写)或数字。



图 13-1-4 配置 AP 无线参数

(3) 通道

IEEE 802.11 标准使用不需要许可的 ISM 无线频段在无线局域网中建立了通道。2.4GHz 频段在北美被细分为 11 个通道，在欧洲被细分为 13 个通道，考试中要以北美的为准，毕竟思科是美国的。每个通道占用 22MHz，相邻的通道相差 5MHz，如图 13-1-5 所示，很多通道之间都出现重叠的频率。在无线局域网中最佳的做法是把 AP 设置在不重叠的通道。如果有 3 个相邻接入点，使用通道 1、6 和 11；如果有两个，选择任何两个间隔 5 个通道的通道都可以，比如通道 2 和 7。许多接入点可以在邻近区域上自动选择一个没有重叠的通道，也有一些产品可以不断监测无线电空间，根据所处环境动态调整所处的通道。

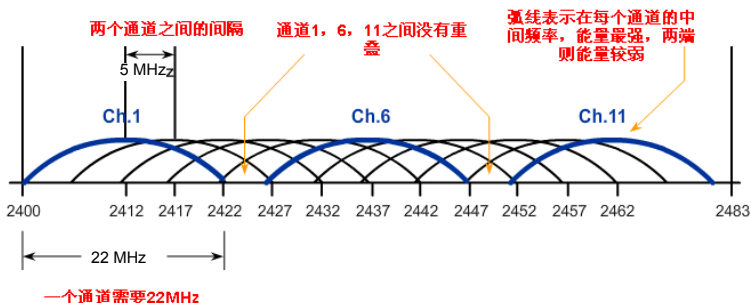


图 13-1-5 2.4GHz 频段的 11 个通道

2. 无线网络拓扑

无线局域网包含多种网络拓扑结构，最基本的网络拓扑结构是 BSS（Basic Service Set，基本服务集）。

(1) Ad hoc

无线网络在没有 AP 的情况下，也可运行，这叫做 Ad hoc 拓扑。配置客户端的无线参数，使它们在 Ad hoc 模式下工作。IEEE 802.11 把这种工作在 Ad hoc 模式下的网络叫做 IBSS（Independent BSS，独立的基本服务集），如图 13-1-6 所示。

(2) BSS

有单一的 AP 参加，无线客户端都连接在 AP 上，这叫做 Infrastructure 拓扑，可提供额

外的服务，增强客户端之间的距离。IEEE 802.11 把这样的无线网络叫做 BSS。BSS 和 IBSS 服务的区域是 BSA（Basic Service Area，基本服务区域），如图 13-1-7 所示。



图 13-1-6 Ad hoc 网络

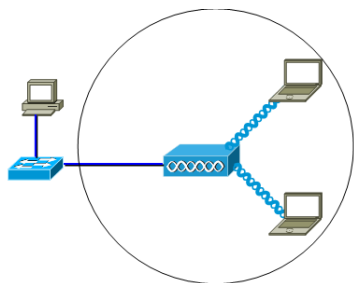


图 13-1-7 BSS 网络

（3）ESS

当一个简单的 BSS 不能提供足够的无线覆盖时，一个或多个 AP 被加入进来，组成一个 ESS（Extended Service Set，扩展服务集），这还叫做 Infrastructure 拓扑，如图 13-1-8 所示。在 ESS 中，一个 BSS 通过 BSSID（BSS Identifier，BSS 标识，也就是服务 BSS 的 AP 的 MAC 地址）来区别于其他的 BSS。ESS 的作用范围是 ESA（Extended Service Area，扩展服务区域）。

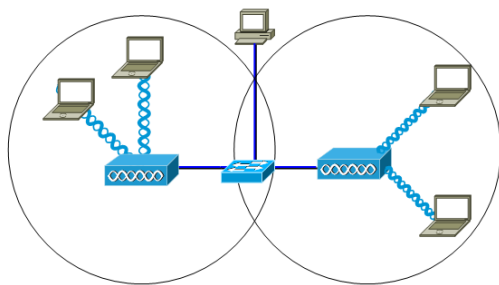


图 13-1-8 ESS 网络

为了便于区分，表 13-1-4 中列出了不同无线拓扑间的比较。

表 13-1-4 无线网络拓扑

无线设备	拓扑模式	拓扑建筑砌块（Topology Building Block）	覆盖范围
没有 AP	Ad hoc	IBSS	BSA
一个 AP	Infrastructure	BSS	BSA
超过一个 AP	Infrastructure	EBSS	ESA

（4）Common Distribution System

Common Distribution System（共同分布系统）允许多个 AP 在一个 ESS 中以 BSS 的方式出现。一个 ESS 一般包括一个共同的 SSID 来允许用户漫游在多个 AP 之间。在两个单元之间有 10%~15% 的覆盖范围重叠，只有一个 SSID，并且使用没有重叠的通道（比如一个单元在通道 1，另一个单元在通道 6）的情况下，可以实现漫游功能。

3. 客户端和 AP 间的连接

802.11 处理的一个关键部分是发现无线局域网，并连接到无线局域网，处理过程包括

以下部分：

- 灯塔（Beacons）：无线局域网用来通告自己存在的帧。
- 控测器（Probes）：无线客户端用来发现网络的帧。
- 认证（Authentication）：身份识别过程。
- 连接（Association）：在 AP 和无线客户端间建立数据链路的过程。

灯塔的主要目的是允许无线客户端了解到在区域内有哪些网络和 AP 可以使用，允许客户端选择要使用的网络和 AP。AP 可以周期性地广播灯塔信号，其实就是发送通告自己存在的帧。802.11 客户端加入网络的步骤如下：

第一步：探测（Probing）。客户端通过在多个通道上发送探测请求来搜索网络，探测请求指定网络的名字（SSID）和可以支持的速率。一般无线客户端会配置想要连接的 SSID，因此无线客户端发出的探测请求包含想要连接网络的 SSID。

如果无线客户端只是简单尝试发现有哪些可以使用的无线网络，它发出的探测请求没有 SSID，这样所有的被配置为允许应答的 AP 都进行响应，但那些被配置为 SSID 禁止广播的 AP 不会响应。

第二步：认证（Authentication）。802.11 最初发展了两种认证机制，第一种叫做开放式认证，即不采用认证；第二种叫做 WEP（Wired Equivalency Protection，有线相当保护）认证，通过在客户端和 AP 上配置共享密钥实现。这种共享 WEP 密钥的方式试图想在无线网络中提供像有线网络一样的安全，但这种认证方式是有缺陷的，不推荐使用这种认证方式。13.2 节专门介绍无线网络的安全技术，里面会提到其他的认证方式。

第三步：连接（Association）。这个阶段确定安全和速率选项，建立无线客户端和 AP 间的数据链路。作为这个阶段的一部分，客户端学习到 BSSID，也就是 AP 的 MAC 地址。AP 会映射一个逻辑端口叫 AID（Association Identifier，连接识别）到无线客户端，这个 AID 就相当于交换机的一个端口，这样 AP 就可以使无线客户端的帧转发出去。

一旦无线客户端和 AP 之间建立了连接，两台设备间的通信就建立起来了。

13.1.5 规划无线局域网*

仔细地规划无线局域网，使之可以最好地利用资源，提供最好的服务。无线局域网可以从相对简单的配置到非常复杂、精细的设计，WLAN 中可以支持的用户数并不是一个简单的计算，要依赖于设施的布局、用户期望的速率。还需要考虑 RF 的覆盖范围，多个 AP 在一个 ESS 中使用没有重叠的通道等。

AP 一般要放置在障碍物的上面，在室内可以考虑在覆盖范围的中心尽量靠近天花板。一般来说要把 AP 安装在合适的位置，比如安装在会议室（conference room）的效果就比安装在走廊（hallway）里的效果好。



13.2 无线局域网安全***

对于任何使用或管理网络的人来说，安全都应该被优先考虑。保护无线网络安全要比保护有线网络安全的难度大，一个无线局域网对一个接入点范围内的每个人开放。利用无线网卡和相关的破解技术，攻击者可能不需要进入工作场所就可以获得无线局域网的访问权。

13.2.1 无线网的安全威胁*

有几类的威胁，导致未经授权的访问：War drivers（驾驶攻击）、Hackers /Crackers（黑客/攻击者）、Employees（雇员）、Rogue Access Points（流氓接入点）、Man-in-the-Middle Attacks（中间人攻击，简称 MITM）和 Denial of Service（拒绝服务，简称 DoS）。

当今出售的很多无线设备都有一个默认设置，用户只需要很少配置或不需要配置就可以使用无线设备了。在很多情况下，用户不更改无线设备的默认设置，也不启用认证或者只启用默认的 WEP 认证，这样很容易造成攻击。

驾驶攻击是指利用带有 802.11b/g 客户端网卡的笔记本电脑扫描邻近区域来寻找不安全的 802.11b/g 系统进行攻击。

流氓接入点攻击是指一个 AP 被放置在无线局域网中用来干扰正常的网络运行。如果一个流氓接入点配置了正确的安全设置，将可以捕获客户的数据。一个流氓接入点也可以经过配置，让未经授权的用户获取 MAC 地址信息，捕捉和伪造数据包，更糟的是可能获得服务器和文件的访问权。一般的流氓接入点，是雇员未经授权安装的。雇员在私自装 AP 打算使用企业网络，这些 AP 通常没有进行必要的安全配置，使网络中存在一个安全漏洞。

MITM（中间人攻击）：黑客并不直接登录用户的网络，而是将它设定成 AP，冒充正常的网络 AP，有着正常的网络 AP 的设置，并发送很强的信号，一般用户将误判断为公司的 AP，并向它发送资料。通过对这些资料的分析，黑客将可能获得有用信息。

DoS：802.11b/g 使用的是 2.4GHz 的频段，这个无线频段也被很多电子消费产品使用，攻击者可以利用这些产品，制造干扰信号；攻击者还可以利用 CSMA/CA 中的 RTS/CTS（要求发送/清除发送）特性不停地发送干扰信号，造成数据发送失败；攻击者也可伪造信号，解除 AP 和客户端的连接，然后大量的客户端再重新连接 AP，造成拥塞。

13.2.2 无线网安全协议**

1. 无线协议

这里介绍一般的无线协议和它们可以提供的安全级别。802.11 最初采用两种验证方式，即开放式和 WEP 方式，开放式就是没有验证，WEP 提供了和有线相当的安全验证，但 WEP 验证本身是有缺陷的，需要进一步改进。很多公司的做法是 cloaking SSID（隐藏 SSID）和 filtering MAC address（过滤 MAC 地址），但这两种方法也有缺陷。

WEP 共享密钥有两方面的缺陷：一是这种加密数据的机制是可以被破解的；二是不容易扩展，很难在大范围内部署。WEP 中的密钥需要手工管理，手工输入，经常出错。

考虑到 WEP 的不足，TKIP（Temporal Key Integrity Protocol，临时密钥完整性协议）加密算法被建立，WPA（WiFi Protected Access，WiFi 保护访问）使用 TKIP 加密方法，其加密特性决定了它比 WEP 更难以入侵。WPA 作为 IEEE 802.11 通用的加密机制 WEP 的升级版，在安全的防护上比 WEP 更为周密，主要体现在身份认证、加密机制和数据包检查等方面。

WPA 与 WEP 不同，WEP 使用一个静态的密钥来加密所有的通信。WPA 不断地转换密钥。WPA 采用有效的密钥分发机制，可以跨越不同厂商的无线网卡实现应用。WPA 的另一个优势是，它使公共场所和学术环境安全地部署无线网络成为可能。而在此之前，这些场所一直不能使用 WEP，WEP 的缺陷在于其加密密钥为静态密钥而非动态密钥，这意味着，

为了更新密钥, IT 人员必须亲自访问每台机器, 而这在学术环境和公共场所是不可能的; 若是让密钥保持不变, 又会使用户容易受到攻击。

802.11i 发布之前, WPA 是最基本的无线安全机制。而 WPA 只解决 802.11i 草案中的部分问题, 也就是改善 WEP 的安全性。802.11i 是由 IEEE 制订的, 它包括两个部分: 一部分用于改进使用当前算法的现有 802.11 设备; 另一部分则使 802.11 设备具备了新的能力, 能够支持高级加密标准(AES)的加密算法。虽然 WPA 比 WEP 更安全, 但它却没有达到 802.11i 的水平。WPA2 是 WiFi 联盟发布的第二代 WPA 标准, 与 WPA 第一代标准兼容。802.11i 和 WPA2 的特性基本上是相同的, 它们的最重要特性是预验证: 在用户对延迟毫无察觉的情况下实现安全快速漫游, 以及采用 CCMP 加密包来替代 TKIP。CCMP (Counter mode with Cipher-block chaining Message authentication code Protocol, 计数器模式及密码区块链信息认证码协议) 是一种基于 AES 的加密机制, AES 可以产生某些企业、政府部门和其他机构所需要的高水平数据隐私能力。CCMP 支持在 802.11i 和 WPA2 中是强制性的, 预验证则是可选内容。

今天, 很多企业都遵循的 802.11i 标准, 与 WPA2 标准相似。WPA 和 WPA2 都有企业和个人标准之分, 对于企业来说, WPA2 需要连接到 RADIUS 数据库, 实施企业级部署。RADIUS 是认证方式, 有专门的 RADIUS 认证服务器, CCNP 课程会介绍到这种认证方式的使用。

2. 认证

在有严格安全要求的网络中, 需要有额外的登录或认证机制。登录过程被 EAP (Extensible Authentication Protocol, 扩展认证协议) 管理, IEEE 使用 802.1x 协议对无线局域网进行认证和授权。

EAP 的认证过程如下:

- ① AP 上的 802.11 连接进程为每个无线局域网的用户创建一个虚拟接口。
- ② AP 阻止所有的数据帧, 除了 802.1x 协议的通信流量。
- ③ 通过 AP, 802.1x 的数据帧携带 EAP 身份验证数据包到达服务器。这台服务器上运行 RADIUS 协议, 可以提供认证、授权和计费, 即 AAA 服务。这里 AP 起到一个中转站的作用, 把服务器的 EAP 要求转发给无线客户端, 把无线客户端的 EAP 应答转发给 AAA 服务器。
- ④ 如果 EAP 的验证是成功的, AAA 服务器发送一个 EAP 的成功信息给接入点, 然后让无线局域网客户端的数据流量通过虚拟接口。
- ⑤ 开放虚拟接口前, WLAN 客户端和 AP 间的数据链路被加密, 以确保没有其他的 WLAN 客户端可以接入只能由已授权认证的客户端接入的端口。

在 802.11i (也就是 WPA2), 甚至 WPA 被使用前, 一些公司试着通过过滤 MAC 地址和不广播 SSID 来增强无线局域网的安全。今天, 很容易地通过软件来修改 MAC 地址, 因此 MAC 地址过滤是很容易被欺骗的。即使 AP 的 SSID 不被广播出去, 其他无线客户端和 AP 间往返的数据也会泄露 AP 的 SSID。如果攻击者被动地监控 RF 频段, SSID 很容易被捕获, 因为 SSID 是明文传输的。通过使用 MAC 地址过滤和不广播 AP 的 SSID 的方法来保护无线网络的安全是不可靠的。在无线局域网上确保用户安全, 最好的方法应该是使用基于端口的网络访问控制, 比如 WPA2。

3. 加密

802.11i 说明的两个企业级的加密机制是由 WiFi 联盟指定的 WPA 和 WPA2。与之相关的加密算法有 TKIP（临时密钥完整性协议）和 AES（Advanced Encryption Standard，高级加密标准）。

TKIP 是 WPA 指定的加密方法，它致力于解决传统 WEP 加密方法的缺陷，它使用的仍然是 WEP 的原始加密机制。TKIP 有两个功能：一是加密第二层的负荷；二是在加密的包中传输 MIC（Message Integrity Check，信息完整性检查），确保信息没有被篡改过。

尽管 TKIP 解决了所有 WEP 已知的不足，但 WPA2 的 AES 加密却更受欢迎，因为给无线局域网带来了主要的 IT 工业标准，最显著的就是 802.11i。AES 和 TKIP 有同样的功能，但它允许目的主机使用发过来的 MAC（Message Authentication Code，信息完整性鉴别），来判断信息没有被篡改过。

在配置 Linksys AP 或无线路由器的时候，可能看不到 WPA 或 WPA2，看到的可能是 PSK（Pre-Shared Key，预共享密钥）之类的选项。各种类型的 PSK 意思如下：

- 使用 TKIP 加密的 PSK 或 PSK2 和 WPA 相同。
- 使用 AES 加密的 PSK 或 PSK2 和 WPA2 相同。
- 没有指定加密方式的 PSK2 也和 WPA2 相同。

13.2.3 加强无线网安全*

通过前一节的介绍，可以使用下面的方法来保护无线局域网的安全：

- ① 关闭 AP 的 SSID 广播功能；
- ② 启用 MAC 地址过滤功能；
- ③ 执行 WPA2 安全。

需要注意的是，方法①和方法②不被认为是一个有效的安全方法。



13.3 配置无线局域网*

本节介绍无线局域网的配置，包括配置 AP 和配置无线网卡。本节在生活中比较实用，但在 CCNA 考试中所占比重不大，动手配置无线局域网有助于加深对本章各节知识的理解和记忆。CCNA 考试中涉及的 AP 产品是 Linksys WRT300N，是一台无线宽带路由器，集成了 AP、交换机、路由器的功能。笔者手边只有一台 Linksys WRT54G 的无线宽带路由器，不同型号的产品会有些功能差异，但不会影响到考试。Linksys WRT54G，以下简称 Linksys。如果读者手边没有 Linksys 无线宽带路由器，可以在 13.3.3 节叙述的 Packet Tracer 模拟器中感受一下 Linksys 的操作。

13.3.1 配置 Linksys**

Linksys 无线宽带路由器是一台可以让用户通过网络连接到 Internet 的设备。它提供了 1 个 Internet 接口、4 个局域以太网接口，另外还提供 11Mb/s 或者 54Mb/s 的无线连接。Linksys 无线宽带路由器同时提供了 802.11b、802.11g 和以太网接口，并且可以让它们互相通信。

1. 选择位置

在配置 Linksys 宽带路由器之前，选择一个较佳的位置和一个没有干扰的无线频道，可

以大大地提高网络的性能。通常最好的位置是网络中央，并在那里可以直线看到所有的无线客户端、固定天线，通常天线放置在较高的位置，可以提高网络接入速率。

2. 连接

将路由器的 Internet 接口连接到 Cable 或 DSL 宽带调制解调器上；电源插口是用来连接电源变压器的；将 PC 或者网络设备连接到路由器背面板上的数字接口上，如果不采用有线，也可使用无线，开启 PC 的无线，搜索到 Linksys 并连接。按 Reset 按钮约 10 秒钟可将路由器设置恢复为出厂默认配置，一般用在忘记密码的情况下。

3. PC 的设定

这里以配置 Windows XP 系统为例，其他操作系统与这里的步骤类似。

① 这里假定 Windows XP 是经典界面，单击“开始”→“设置”→“控制面板”，在“控制面板”窗口中双击“网络和拨号连接”图标。

② 在“网络连接”窗口中，双击“本地连接”或“无线网络连接”图标，单击“属性”按钮，如图 13-3-1 所示。

③ 选择对话框中的“Internet 协议 (TCP/IP)”，并单击“属性”按钮。在“Internet 协议 (TCP/IP) 属性”窗口中，选择“自动获得 IP 地址”，单击两次“确定”按钮，完成配置，如图 13-3-2 所示。

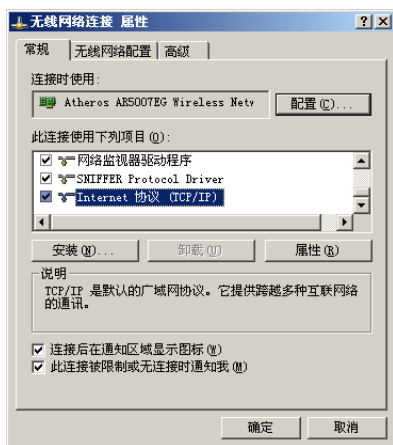


图 13-3-1 无线网络连接属性

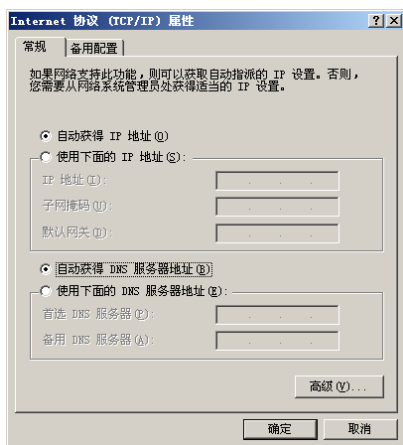


图 13-3-2 配置 IP 地址

4. 连接 Linksys

Linksys 出厂时已经做好设定，可以立即使用它。当然，如果需要变动任何设定值，都可以通过网页进行更改。在 PC 浏览器的地址栏中输入 192.168.1.1（这是路由器预设的 IP 地址，路由器默认还启用了 DHCP，设成自动获取后，PC 会从路由器获取到 192.168.1.0/24 的 IP 地址），在弹出的身份验证窗口的用户名中输入“admin”，在密码中输入“admin”，路由器的预设密码是“admin”，出于安全考虑，请用户更改密码。打开 Linksys 的管理界面，如图 13-3-3 所示。

- **设置：**包括基本设置、DDNS、MAC 地址克隆和高级路由等。一般只需要配置“基本设置”即可，在“基本设置”中可以选择接入 Internet 的方式，并输入 ISP 运营商

提供的资料, 还可设定本地局域网段的 IP 地址, 默认的是 192.168.1.1/24, 可以根据需要调整 IP 地址。要记住的是, 如果路由器的 IP 地址更改了, 路由器 DHCP 服务器提供的 IP 地址范围也要随之改变。

- **无线:** 后面专门介绍。
- **安全性:** 包括防火墙和 VPN 的设置, 一般保持默认即可, 本书不作介绍。
- **访问限制:** 主要是 Internet 访问策略的设置, 和本书后面要提到的 ACL (访问控制列表) 类似, 本书不作介绍。
- **应用程序&游戏:** 配置端口转发、DMZ (Demilitarized Zone, 中文名称为“隔离区”, 也称“非军事化区”)、QoS (Quality of Service, 服务质量) 等, 本书不作介绍。
- **管理:** 包括管理、日志、诊断、出厂默认值、固件升级、配置管理等, 其中最主要的管理子项, 可以设置路由器的密码, 建议修改默认的管理密码“admin”为其他值。
- **状态:** 包括路由器、本地网络和无线的状态查询。

5. 无线

无线设置部分包括: 基本无线设置、无线安全性、无线 MAC 筛选器和高级无线设置。

(1) 基本无线设置

基本无线配置包括无线网络模式、无线网络名称 (SSID)、无线通道和无线 SSID 广播等, 如图 13-3-4 所示。



图 13-3-3 Linksys 的管理界面



图 13-3-4 基本无线配置

- **无线网络模式:** 无线网络模式有 4 个选项, 可以从下拉框中选择。分别是:
 - 禁用: 不开启 Linksys 的无线功能;
 - 混合: 既支持 802.11b, 又支持 802.11g 的无线客户端;
 - 仅限 B: 只支持 802.11b 的无线客户端;
 - 仅限 G: 只支持 802.11g 的无线客户端。
- **无线网络名称 (SSID):** 也就是 Linksys 的名称, 可以改成一个更直观的名称, 如果是多台无线 AP 提供漫游支持, 需要将所有 AP 的名称设成一样。
- **无线通道:** 图 13-1-5 提到每个通道占用 22MHz, 相邻通道间相差 5MHz, 在北美只

有 11 个通道，在欧洲有 13 个通道，中国使用的也是 13 个通道。为了不相互影响，相邻的 AP 不要使用有重叠的通道，比如相邻有三个 AP，可以使用 1、6、11 通道。Linksys 默认使用的是通道 6。

- **无线 SSID 广播：**包括启用或禁用，这也就是前面提到的隐藏 AP 的 SSID，如果 AP 不广播 SSID，就需要在无线客户端静态设置 AP 的 SSID 等连接信息。要知道，仅禁用无线 SSID 广播是不能完全保护无线网络安全的，因为黑客可以通过捕获其他用户的通信包来获知 AP 的 SSID，SSID 采用的是明文传输。

(2) 无线安全性

Linksys 默认没有启用无线安全性，用户可以从安全模式下拉框中选择所需的安全模式，然后单击“保存设置”按钮，如果要放弃更改，请单击“取消更改”按钮，放弃本次操作，如图 13-3-5 所示。

- **禁用：**就是不使用安全性，也就是前面提到的开放式。
- **WEP：**无线安全最初的一个协议，是一种基本加密方法，不如 WPA 安全，WEP 的密钥是固定的，除非手动改变，不利于大范围部署，如图 13-3-6 所示。



图 13-3-5 无线安全模式



图 13-3-6 WEP 模式

读者可以在“密钥 1”栏中直接输入密钥，记住图 13-3-6 中选择的是“10 个十六进制数字-64 位加密”，所以输入的要 10 位十六进制数。“密钥 2”、“密钥 3”和“密钥 4”栏中也可以输入密钥，比如以后想更换成密钥 2，只需把“默认传输密钥”选成 2 就可以了，但笔者在实验过程中却发现只有使用默认传输密钥 1 才可以。如果读者嫌手工输入 4 组密钥太麻烦，可以随便在“密码”栏中输入些什么内容，然后单击“生成”按钮，会自动生成 4 组密钥。如图 13-3-6 所示，在“密码”栏中输入“qwerty”，单击“生成”按钮，下面就自动生成了 4 组密钥。这里要问读者的是，客户端连接时，提示输入密钥，应该输入哪一个呢？正确的答案是输入“A2FE9FCC88”，不区分大小写，“qwerty”并不是要输入的密钥。除非手工改变，“A2FE9FCC88”这个密钥将一直有效，并且使用的就是“A2FE9FCC88”这个密钥。

- **RADIUS：**WEP 用于与 RADIUS 服务器协调工作（这种方法只能用于 RADIUS 服务器已经连接到这台路由器的时候）。首先，输入 RADIUS 服务器地址和端口号，然后再输入验证路由器与服务器之间共享的密钥，最后再输入 WEP 密钥，如图 13-3-7 所示。
- **WPA Personal：**WPA Personal 有两种加密方法，即 TKIP 和 AES，使用动态密钥，请选择一种加密算法，然后输入一个 8~63 字符的共享密钥，最后输入组密钥更新的时间，这是路由器更换密钥的周期，如图 13-3-8 所示。

安全模式:

RADIUS 服务器地址:

RADIUS 端口:

共享密钥:

默认传输密钥: ☒ 1 ☐ 2 ☐ 3 ☐ 4

WEP 加密:

密码:

密钥 1:

密钥 2:

密钥 3:

密钥 4:

图 13-3-7 RADIUS 模式

安全模式:

WPA 算法:

WPA 共享密钥:

组密钥更新: 秒

图 13-3-8 WPA Personal 模式

在图 13-3-8 中, AP 端设置的密钥是“qwertyui”, 客户端配置的密钥也是“qwertyui”, 读者不仅要问, 这和 WEP 相比, 感觉没有什么差别呀? 既然只有一个密钥, 如何周期性更新呀? 其实在 WPA 中使用的并不是“qwertyui”, 而是两端在共同信息“qwertyui”的基础上协商出来的另一个密钥, 两端可以周期性地再协商, 不停地更换密钥。而 WEP 使用的却始终是设置的那个密钥。

- **WPA Enterprise:** WPA 用于与 RADIUS 服务器协调工作(这种方法只能用于 RADIUS 服务器已经连接到这台路由器的时候), 如图 13-3-9 所示。首先, 输入 RADIUS 服务器地址和端口号, 然后再输入验证路由器与服务器之间共享的密钥, 最后再输入更新周期。
- **WPA2 Personal:** WPA2 Personal 有两种加密方法, 即 TKIP+AES 和 AES。使用动态密钥, 请选择一种加密算法, 然后输入一个 8~63 字符的共享密钥, 最后输入组密钥更新的时间, 这是路由器更换密钥的周期。
- **WPA2 Enterprise:** WPA2 用于与 RADIUS 服务器协调工作。首先, 输入 RADIUS 服务器地址和端口号, 然后再输入验证路由器与服务器之间共享的密钥, 最后再输入更新周期。

(3) 无线 MAC 筛选器

无线访问可以通过 MAC 地址过滤来控制, 这也就是前面提到的 MAC 地址过滤技术, 和禁用 SSID 广播一样, 都不能提供完全的安全保障, 只能起到安全的辅助作用, 如图 13-3-10 所示。现在有很多应用程序可以修改 MAC 地址, 这种方法基本起不到保护作用。

安全模式:

WPA 算法:

RADIUS 服务器地址:

RADIUS 端口:

共享密钥:

密钥更新超时: 秒

图 13-3-9 WPA Enterprise 模式

设置	无线	安全性	访问限制	应用程序 & 游戏
基本无线设置	无线安全性	无线 MAC 筛选器	高级无线设	

无线 MAC 筛选器: ☒ 启用 ☐ 禁用

防止: ☒ 防止列出的 PC 访问无线

只允许: ☐ 只允许列出的 PC 访问无线网络

图 13-3-10 无线 MAC 筛选器

13.3.2 配置无线网卡*

双击任务栏上或网络连接窗口中的无线网络连接图标，打开“无线网络连接状态窗口”，如图 13-3-11 所示。

1. 搜索可用无线网络

单击图 13-3-11 中的“查看无线网络”按钮，打开如图 13-3-12 所示的“无线网络连接”窗口，选中一个没有连接的 AP，单击“连接”按钮进行连接；选中一个已连接的 AP，单击“断开”按钮放弃连接。如果是启用了安全的无线网络，还需要提供相应的密码。图中的 linksys 和 dd-wrt 没有启用安全，dlink 启用了 WPA2 的安全无线网络，TP-LINK 也是启用了安全的无线网络。

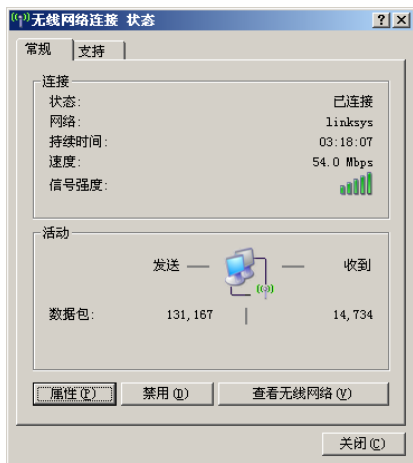


图 13-3-11 “无线网络连接状态”窗口



图 13-3-12 “无线网络连接”窗口

2. 更改首选网络的顺序

如果需更改计算机连接 AP 的优先顺序，单击图 13-3-12 中的“更改首选网络的顺序”链接，打开如图 13-3-13 所示的“无线网络连接属性”窗口的“无线网络配置”标签。在“首选网络”列表框中选择对应的 AP，然后单击“上移”或“下移”按钮，更改它们的顺序。

3. 添加网络

如果 AP 禁用了 SSID 广播，它不会出现在图 13-3-12 中。这时就需要在无线客户端手工添加 AP 的信息。单击图 13-3-13 中的“添加”按钮，打开如图 13-3-14 所示的“无线网络属性”窗口，在“网络名 (SSID)”中填入 AP 的 SSID，比如填入“baomi”；并选中“即使此网络未广播，也进行连接”复选框；在“无线网络密钥”区域中选择正确的网络身份验证方式和相应密钥信息。单击“确定”按钮，完成无线网络的添加。

4. Ad hoc 网络配置

Ad hoc 网络也就是计算机到计算机的网络，没有使用 AP。比如两台笔记本电脑都配置了无线网卡，可以不通过 AP 直接相连。在图 13-3-14 中，随便添加一个网络名 (SSID)，然后选中“这是一个计算机到计算机 (特定的) 网络；没有使用无线访问点”复选框。再

次查看无线网络，可以发现刚添加的网络名（SSID），两台笔记本电脑都连接到这个 SSID，并配置正确的 IP 地址，就可以正常通信了。

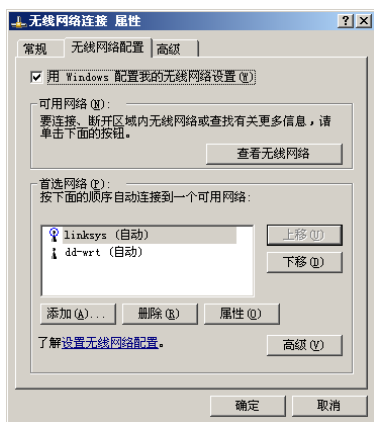


图 13-3-13 更改“首选网络”的顺序

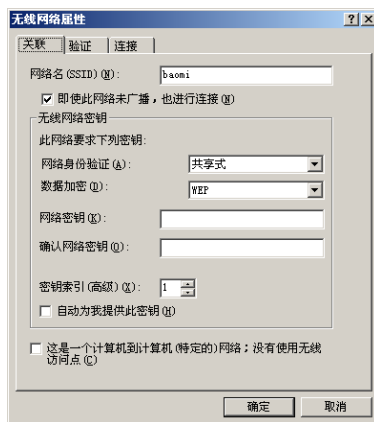


图 13-3-14 “无线网络属性”窗口（添加无线网络）

13.3.3 Packet Tracer 中配置 Linksys*

从 Packet Tracer 模拟器的“Wireless devices”中拖入 Linksys，然后从“End devices”中拖入一台 PC。PC 默认配置的是有线网卡，关闭 PC 的电源，把有线网卡拖回“MODULES”列表中，选择“Linksys-WMP300N”，把该无线网卡拖到计算机的插槽中，如图 13-3-15 所示。

打开计算机的电源，可以看到 PC 与 Linksys 之间已经建立了无线连接，如图 13-3-16 所示。

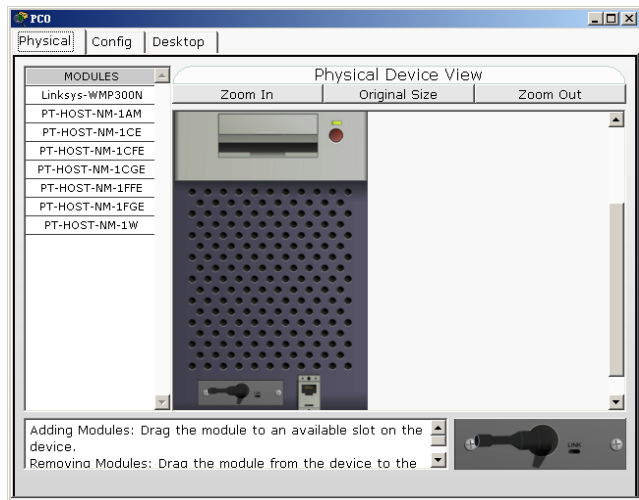


图 13-3-15 给 PC 配置无线网卡

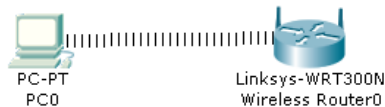


图 13-3-16 无线连接

打开 PC 的“Desktop”标签，打开 Web Browser，在 IE 地址栏中输入“http://192.168.1.1”，弹出验证窗口，在用户名和地址栏中都输入 admin，打开 Linksys 的管理界面，如图 13-3-17 所示。

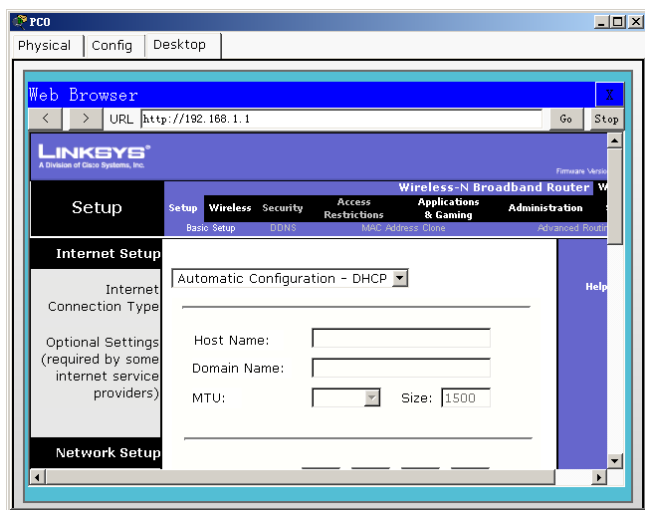


图 13-3-17 在 Packet Tracer 模拟器中配置 Linksys

读者可以在如图 13-3-17 所示的界面中对 Linksys 进行配置。模拟 Linksys 的功能有限，但可以进行一些常用的配置，也支持 WEP 认证实验。如果 Linksys 上配置了 WEP 验证，PC 上也要配置 WEP 验证，PC 上配置 WEP 的界面如图 13-3-18 所示。

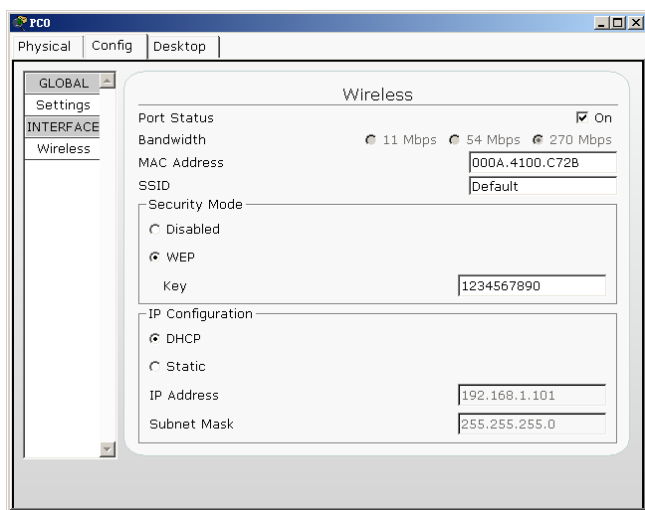


图 13-3-18 PC 上配置 WEP 的界面



13.4 无线故障排除**

无线局域网故障排除也需要一个系统化的方法，那就是从下层的物理层到上层的应用层。无线网络的一些排错步骤和有线网络相同，本节只介绍可能出现的与无线有关的问题。

1. 排除计算机的问题

计算机端可能出现的问题有：

(1) **无线网卡**。有时可能需要尝试不同的无线网卡，这种可能出现的概率很小。如有

必要，可以重新安装驱动程序或升级驱动程序。

(2) **无线网卡设置不正确**。如果无线网卡的客户端不工作，检查安全模式和加密设置。如果安全设置不匹配，客户端无法访问无线局域网。

(3) **效果不好**。如果无线客户端可以访问，但效果不好，可以检查下列项目：PC 与 AP 间有多远，有没有超出计划的覆盖面积范围；检查在客户端通道设置，只要 SSID 是正确的，客户端软件应该会侦测到适当的通道；在该地区运行 2.4GHz 频段的其他设备，比如无绳电话、婴儿监视器、微波炉、无线安全系统，以及潜在的无赖 AP，这些设备都会造成干扰，在无线局域网中造成客户端和 AP 之间间歇性方面的问题。

2. 不正确的通道设置 (Incorrect Channel Settings)

如果用户反映的连接问题出现在 ESS (有多个 AP 的区域)，有可能是通道设置问题。今天有多数无线局域网运行在 2.4GHz 频段，可以有多达 14 个通道，每个通道占用 22MHz 的带宽。能量不是平均分布在整个 22MHz，通道的中心频率能量最强，通道的边缘能量减弱。如果通道有重叠，就可能会发生干扰。如果通道的中心频率接近，情况会更糟，但即使只有轻微的重叠，信号也会互相干扰。可以设定不同 AP 的通道，间隔 5 个通道，如通道 1、通道 6 和通道 11。

3. 无线电频率干扰 (RF Interference)

有些无线电频率干扰来自工作场所或家中，比如无绳电话、婴儿监视器，以及微波炉等。有些消费产品可能没有占用固定的通道，但它们占用了一定的频宽。一般建议把 AP 调在通道 1 或 6，因为很多消费产品默认使用的就是通道 6，比如无绳电话使用的就是通道 6。有条件的话，可以借助专门的工具和软件来检测，Airmagnet 就是一款探测工具。

4. AP 位置不当 (AP Misplacement)

有时丢失到 AP 的连接或数据速率比应该有的速率慢很多，可能的原因有两个：一是距离太远，超出了 AP 的覆盖范围；二是 AP 天线的方向不对，比如指向了走廊 (hallways) 或角落 (corners)。

保证 AP 覆盖区域至少重叠 10%~15%，还要注意 AP 的摆放位置和方向，比如放置在障碍物的前面，尽量放置在覆盖范围的中央接近天花板的地方，尽量放置在空旷的地方（放在会议室的效果要比放在走廊中好）。

还有一些额外的有关接入点和天线位置的具体细节如下：

- 确保 AP 与人的身体相距超过 20 厘米；
- AP 周围 91.4 厘米处不要安放金属障碍物；
- AP 要远离微波炉，微波炉和 AP 使用同样的频率，并可产生信号干扰；
- AP 的天线要垂直摆放；
- 不要把 AP 安装在建筑物的外面；
- 不要将 AP 安装在建筑物周边的墙壁上，除非打算覆盖室外的范围。

5. 认证和加密问题

WLAN 中最有可能遇到的是认证和加密问题。如果 AP 配置了一种类型的加密，客户端提供了另一种不同类型的加密，则身份验证过程失败。所有连接到同一个 AP 的设备必须使用和 AP 相同的安全类型号。



13.5 真题精选***

1. What is the maximum data rate specified for IEEE 802.11b WLANs?

- A. 10Mb/s B. 11Mb/s C. 54Mb/s D. 100Mb/s

2. Which spread spectrum technology does the 802.11b standard define for operation?

- A. IR B. DSSS C. FHSS
D. DSSS and FHSS E. IR, FHSS and DSSS

3. Three access points have been installed and configured to cover a small office.

What term defines the wireless topology?

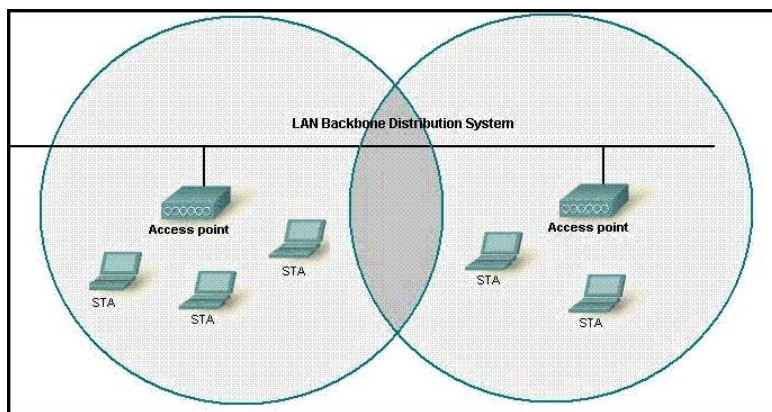
- A. BSS B. IBSS C. ESS D. SSID

4. Which wireless LAN design ensures that a mobile wireless client will not lose connectivity when moving from one access point to another?

- A. using adapters and access points manufactured by the same company
B. overlapping the wireless cell coverage by at least 10%
C. configuring all access points to use the same channel
D. utilizing MAC address filtering to allow the client MAC address to authenticate with the surrounding APs

5. Refer to the exhibit. What two facts can be determined from the WLAN diagram?

(Choose two.)



- A. The area of overlap of the two cells represents a basic service set (BSS).
B. The network diagram represents an extended service set (ESS).
C. Access points in each cell must be configured to use channel 1.
D. The area of overlap must be less than 10% of the area to ensure connectivity.
E. The two APs should be configured to operate on different channels.

6. You and a co-worker have established wireless communication directly between your wireless laptops. What type of wireless topology has been created?

- A. BSS B. ESS C. IBSS D. SSID

7. Which two statements best describe the wireless security standard that is defined by WPA? (Choose two.)

- A. It specifies use of a static encryption key that must be changed frequently to enhance security.
- B. It requires use of an open authentication method.
- C. It specifies the use of dynamic encryption keys that change each time a client establishes a connection.
- D. It requires that all access points and wireless devices use the same encryption key.
- E. It includes authentication by PSK.

8. What is one reason that WPA encryption is preferred over WEP?

- A. A WPA key is longer and requires more special characters than the WEP key.
- B. The access point and the client are manually configured with different WPA key values.
- C. WPA key values remain the same until the client configuration is changed.
- D. The values of WPA keys can change dynamically while the system is used.

9. Which encryption type does WPA2 use?

- A. AES-CCMP
- B. PPK via IV
- C. PSK
- D. TKIP/MIC

10. Which additional configuration step is necessary in order to connect to an access point that has SSID broadcasting disabled?

- A. Set the SSID value in the client software to public.
- B. Configure open authentication on the AP and the client.
- C. Set the SSID value on the client to the SSID configured on the AP.
- D. Configure MAC address filtering to permit the client to connect to the AP.

11. Which two devices can interfere with the operation of a wireless network because they operate on similar frequencies? (Choose two.)

- A. copier
- B. microwave oven
- C. toaster
- D. cordless phone
- E. IP phone
- F. AM radio

12. Which two practices help secure the configuration utilities on wireless access points from unauthorized access? (Choose two.)

- A. assigning a private IP address to the AP
- B. changing the default SSID value
- C. configuring a new administrator password
- D. changing the mixed mode setting to single mode
- E. configuring traffic filtering

13. A single 802.11g access point has been configured and installed in the center of a square office. A few wireless users are experiencing slow performance and drops while most users are operating at peak efficiency. What are three likely causes of this problem? (Choose three.)

- A. mismatched TKIP encryption
- B. null SSID
- C. cordless phones
- D. mismatched SSID
- E. metal file cabinets
- F. antenna type or direction



13.6 真题解答***

1. 解：B

题目问：802.11b 指定的最大传输速度是多少？参阅本章的表 13-1-3，一目了然。

2. 解：B

题目问：802.11b 采用的是什么样的调制技术？参阅本章的表 13-1-3，一目了然。

3. 解：C

题目问：3 个 AP 被安装，范围覆盖一个小办公室。这种无线拓扑用什么术语说明？参阅本章的表 13-1-4，不使用 AP 的是 IBSS，有一个 AP 的是 BSS，有一个以上 AP 的是 ESS。

4. 解：B

题目问：哪一种无线设计确保一个移动的无线从一个 AP 移动到另一个 AP 而不会丢失连接？其实题目说的就是漫游，漫游要满足三个条件：一是所有的 AP 配置一样的 SSID；二是不同 AP 覆盖的区域至少要重叠 10%~15%；三是不同的 AP 不能使用有重叠的通道。A 选项说使用同一家厂商生厂的网卡和 AP；B 选项说无线单元的覆盖区域至少要 10%；C 选项说所有的 AP 要配置在相同的通道；D 选项说使用 MAC 地址过滤功能，允许周围 AP 验证过的 MAC 地址。只有 B 选项正确。

5. 解：BE

题目问：参照图，从无线图表中可以得出哪两个事实？图中有两个 AP，可以得出 A 选项错，B 选项对。该题考的也是无线漫游问题，C 选项说两个 AP 都要使用通道 1；D 选项说为了确保连接的可靠性，重叠区域必须要小于 10%；E 选项说这两个 AP 将被配置在不同的通道中，结合无线漫游的条件，E 选项正确。故 B 和 E 正确。

6. 解：C

题目问：你和同事的两台膝上（笔记本）电脑直接建立无线连接，这样创建的是什么类型的无线拓扑？没有使用 AP 的无线网络是 Ad hoc 网络，是 IBSS 拓扑。

7. 解：CE

题目问：哪两个语句最好地描述了 WPA 定义的无线安全标准？A 选项说它指定使用一个静态的密钥，为了增强安全，密钥必须被经常改变。A 选项说的是 WEP 协议的特点，WPA 可以周期性地更改密钥；B 选项说它要求使用一个开放式的验证方法。开放式验证就是不采用验证，是早期 WEP 的验证方式之一，WPA 采用的是 TKIP 或 AES 加密；C 选项说每次和客户端建立连接时，动态密钥都会改变。WPA 的密钥是在每次建立连接时动态生成的，就算连接不断开，密钥也会周期性地重新生成；D 选项说它要求所有的无线 AP 和无线设备使用同样的密钥。每个无线客户端只要与所连 AP 的验证方式、验证密钥相同就可以了，而不是所有无线设备；E 选项说它包含了预共享密钥。WPA 使用预共享密钥或 RADIUS 验证。经过上面的分析，故 C 和 E 正确。

8. 解：D

题目问：WPA 加密被 WEP 更受优选的原因是什么？WPA 密钥的长度介于 8 和 63 个字符之间，WEP 的密钥可以是 10 个或 16 个十六进制数，WPA 的密钥也不是一定比 WEP 的

长, 故 A 选项错误; B 选项说 AP 和客户端之间是手工配置使用不同的 WPA 密钥。WPA 中每个客户连接到 AP 都会动态生成一个不同的密钥, 这个密钥是动态生成的, 不是手工配置的; C 选项说 WPA 的密钥不会变直到客户端配置被改变。WPA 的密钥会周期性改变; D 选项说当使用 WPA 的时候, WPA 的密钥能够动态改变。故只有 D 正确。

9. 解: A

题目问: WPA2 使用是什么类型的加密? 本章 13.2.2 节中介绍到 WPA2 使用的是 AES 的加密, CCMP 在 WPA2 和 802.11i 中被强制执行。故正确答案是 A。

10. 解: C

题目问: 为了连接到禁用了 SSID 广播的 AP, 必须额外配置什么? 本章 13.3.2 节介绍了当 AP 禁用 SSID 广播时, 无线客户端需手工添加 AP 的 SSID 和相关信息。而不是选项 A 中说的, 添加的 SSID 是 “public”, 也不是 B 选项中说的配置验证, 更不是 D 选项中说的配置 MAC 地址过滤。故正确答案是 C。

11. 解: BD

题目问: 哪两个设备能干扰无线网络的使用, 因为它们工作在相似的频率上(选 2 个)? 限于知识有限, CCNA 考生不可能具备这样全面的知识, 也不可能了解美国有哪些无线产品, 但只要牢记 3 个答案: baby monitors (婴儿监视器)、cordless phones (无绳电话) 和 microwave ovens (微波炉) 就可以了, 因为这 3 个选项是思科列举出来的典型代表。

12. 解: CE

题目问: 哪两种做法用来阻止无线 AP 上的有用配置来自于没有授权的访问? 在有线网络中, 内网中的主机配置一个私有 IP 地址, 外网就没法访问了, 可是 AP 是提供无线服务的, 只要在无线网络的覆盖范围内, 用户就可以访问到 AP, 因此 A 选项说分配一个私有 IP 地址给 AP 是没有办法起到保护作用的。B 选项说改变默认的 SSID, 如果只是改变而没有禁用 SSID 广播, 无线设备很容易就可发现。C 选项说配置一个新的管理员密码是可行的, 一般厂家的设备都会有一个默认的管理密码, Linksys 默认的是 “admin”, 如果不修改, 很容易就会造成信息泄密。D 选项说改变混合模式为单一模式与本题的问题无关, 混合模式和单一模式是针对 802.11b 和 802.11g 标准的。E 选项说配置流量过滤是可行的, 比如过滤非法的 MAC 地址, 只允许合法的 MAC 地址访问 AP。故正确答案是 C 和 E。

13. 解: CEF

题目问: 一个工作在 802.11g 单一模式的 AP 被安装在一个正方形办公室的中央。当多数用户都工作在峰值速率的时候, 一个新来的无线用户的速率却很慢, 造成这种问题的 3 个可能原因是什么(选 3 个)? 故障的现象是速率慢, 不是不能使用, 这很可能是受到了干扰。针对本题, 可以使用排除法, 选择最可能的 3 个选项。A 选项说加密方式不匹配, 如果加密方式不匹配, 根本就使用不了无线网络, 而不是效率低的问题, 故 A 选项错。B 选项说空的 SSID, 无线访问是需要 SSID 的, 没有 SSID, 无线连接失败, 故 B 选项错。C 选项说无绳电话, 这是一个正确答案, 无绳电话使用的也是 2.4GHz 频段, 极易造成干扰, 引起性能下降, 可能新来的无线用户附近有一台无绳电话, 故 C 选项对。D 选项说不匹配的 SSID, 如果 SSID 不匹配, 无线连接也会失败, 故 D 选项错。E 选项说金属文件柜, 这也是一个正确的答案, 因为金属文件柜可能屏蔽了部分 AP 的无线电信号, 新来的无线用户附近很可能有一个金属文件柜。F 选项说天线方向, 如果 AP 使用的不是全向天线, 新来的无线用户可能处在天线能量不强的方向上, 故 F 选项正确。

第 14 章

广域网**

当企业增长到超过单一的地理位置的时候，就需要互连各个地区的 LAN，形成企业广域网（Wide Area Network，WAN）。本章将讨论广域网关键的技术概念、可用的广域网连接类型。



14.1 广域网概述**

广域网借助服务提供商或运营商（如电话或电缆公司）提供的设施来实现组织内部场所之间、与其他组织场所、外部服务，以及远程用户的互连。广域网通常可以传输各种各样的通信类型，比如语音、数据和视频。

14.1.1 广域网设备*

根据定义，广域网连接相隔较远的设备，这些设备包括：

- 路由器（Router）：提供诸如局域网互连、广域网接口等多种服务，包括 LAN 和 WAN 的设备连接端口。
- WAN 交换机（Switch）：连接到广域网上，进行语音、数据及视频通信。WAN 交换机是多端口的网络设备，通常进行帧中继、X.25 等流量的交换。WAN 交换机通常在 OSI 参考模型的数据链路层之下运行。
- 调制解调器（Modem）：包括针对各种语音级服务的不同接口。信道服务单元/数字服务单元（CSU/DSU）是 T1/E1 服务的接口。终端适配器/网络终结器（TA/NT1）是综合业务数字网（ISDN）的接口。
- 通信服务器（Communication Server）：汇集拨入和拨出的用户通信。

14.1.2 广域网拓扑***

广域网工作在 OSI 七层模型的第一层和第二层，常见的拓扑如图 14-1-1 所示。图中列出描述物理 WAN 连接时常用的术语，包括：

用户驻地设备（Customer Premises Equipment，CPE）：位于用户驻地的设备和内部布线，用户驻地设备连接到运营商的电信信道。用户可以从服务提供商处购买 CPE 或租用 CPE。

数据通信设备（Data Circuit-termination Equipment，DCE）：也称为数据电路终端设备，DCE 由将数据放入本地环路的设备组成。DCE 主要提供一个接口，用于将用户连接到 WAN 网上的通信链路。

数据终端设备（Data Termination Equipment，DTE）：传送来自客户网络或主机的数据

以便在 WAN 上传输的客户设备。DTE 通过 DCE 连接到本地环路。

分界点 (Demarcation Point): 大楼或园区中设定的某个点, 用于分隔客户设备和服务提供商设备。在物理上, 分界点是位于客户驻地的接线盒, 用于将 CPE 电缆连接到本地环路。分界点通常位于技工容易操作的位置。分界点是连接责任由用户转向服务提供商的临界位置。这一点非常重要, 因为出现问题时, 有必要确定究竟是由用户还是服务提供商负责排除故障或修复故障。

本地环路 (Local Loop): 将用户驻地的 CPE 连接到服务提供商中心局的铜缆或光纤电话电缆。本地环路有时也叫做“最后一公里”。

中心局 (Central Office, CO): 本地服务提供商的设备间或设备大楼, 本地电话电缆在此通过交换机和其他设备系统连接到全数字长途光纤通信线路。

最常见的 DCE 设备是 Modem, 最常见的 DTE 设备是路由器。DCE 和 DTE 之间的区别是: DCE 一方提供时钟, DTE 不提供时钟, 但它依靠 DCE 提供的时钟工作, 比如 PC 和 Modem 之间。数据传输通常是经过 DTE 到 DCE, 再经过 DCE 到 DTE 的路径。

在实验室环境中, 通过两台路由器背靠背连接起来模拟广域网, 两台路由器中的一台作为 DCE, 另一台作为 DTE, 做 DCE 的路由器接口下需要配置 clock rate, 提供时钟频率, 不然数据链路层出现故障, 网络层不能正常通信。一些较新的路由器可以检测接口连接线缆的类型, 并自动配置时钟参数。

在 Packet Tracer 模拟器中, 拖入两台 1841 路由器, 并给路由器添加 WIC-2T 模块, 该模块集成了两个串行接口, 读者可以把配置了串行模块的路由器添加到自定义设备中, 这样就不用每次使用到串行接口, 都需要添加模块了。再拖入一根串行线缆, 连接两台路由器的 Ser0/1/0 接口, 如图 14-1-2 所示。

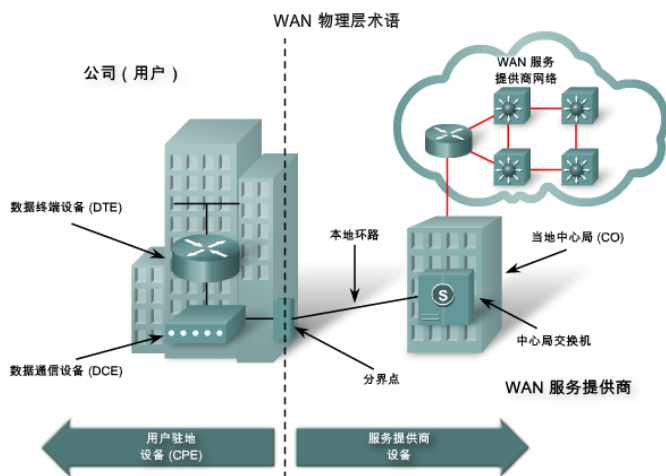


图 14-1-1 广域网连接拓扑

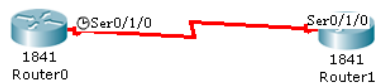


图 14-1-2 实验室中的广域网连接

配置两台路由器接口的 IP 地址, 命令如下:

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s0/1/0
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
```

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s0/1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
```

在 R1 上 ping R2 的 IP 地址 12.1.1.2, 测试网络的连通性, 结果失败。使用“show interfaces serial 0/1/0”命令, 查看接口的状态, 显示如下:

```
R1#show interfaces serial 0/1/0
Serial0/1/0 is up, line protocol is down (disabled)
```

提示协议是 Down 的, 串行线路与以太网链路不同, 需要配置时钟来进行同步。可以使用“show controllers serial 0/1/0”命令查看路由器接口的线缆类型, 显示如下:

```
R1#show controllers serial 0/1/0
Interface Serial0/1/0
Hardware is PowerQUICC MPC860
DCE V.35, no clock
```

在路由器 R2 上查看, 显示如下:

```
R2#show controllers serial 0/1/0
Interface Serial0/1/0
Hardware is PowerQUICC MPC860
DTE V.35 clocks stopped.
```

使用下面的命令, 配置路由器 R1 S0/1/0 接口的时钟参数:

```
R1(config)#int s0/1/0
R1(config-if)#clock rate 64000
```

在串行线缆 DCE 端配置时钟, 64000 是推荐配置的时钟参数。

路由器控制台出现“%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up”, 提示协议也 UP 了, 再次测试 R1 到 R2 的连通性, 可以成功 ping 通。

14.1.3 广域网链路的类型**

常见的广域网链路类型有专线 (Dedicated)、包交换 (Packet Switched) 和电路交换 (Circuit Switched), 如图 14-1-3 所示。

1. 专线

专线是一条专用的点对点链路, 链路带宽和安全都有保障。但专线对每一个目标都需要有一条单独的线路, 花费的成本较高。封装的协议可以是 HDLC、PPP 或 SLIP。

2. 电路交换

电路交换使用的链路是传统的电话网络, 封装协议可以是 PPP、SLIP 或 HDLC。电路交换需要经历三个过程:

- (1) 电路建立。在传输任何数据之前, 要先经过呼叫过程建立一条端到端的电路。
- (2) 数据传输。电路建立以后, 数据可以发送, 在整个数据传输过程中, 所建立的电路必须始终保持连接状态。
- (3) 电路拆除。数据传输结束后, 由某一方发出拆除请求, 然后断开链路。

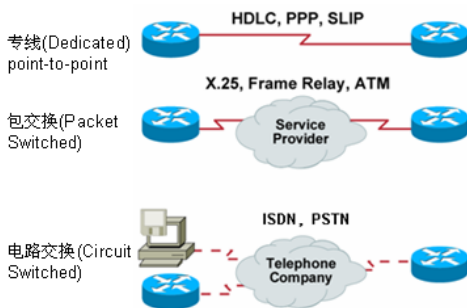


图 14-1-3 广域网链路类型

电路交换技术的优点：数据传输可靠、迅速，数据不会丢失且保持原来的序列。

电路交换技术的缺点：在某些情况下，电路空闲时的信道容易被浪费。在短时间数据传输时，电路建立和拆除所花费的时间很不合算。

电路交换技术的特点：在数据传送开始之前必须先设置一条专用的通道。在线路释放之前，该通道由一对用户完全占用。对于突发式的通信，电路交换效率不高。

3. 包交换

包交换也称分组交换，帧的封装类型可以是 X.25、Frame Relay（帧中继）或 ATM 等。

电路交换技术主要适用于传送话音相关的业务，这种网络交换方式对于数据业务而言，有着很大的局限性。首先，数据通信具有很强的突发性，峰值比特率和平均比特率相差较大，如果采用电路交换技术，按峰值比特率分配电路带宽，则会造成资源的极大浪费；按照平均比特率分配带宽，则会造成数据的大量丢失。其次，和语音业务比较起来，数据业务对时延没有严格的要求，但需要进行无差错的传输，而语音信号可以有一定程度的失真，但实时性一定要高。

分组交换技术就是针对数据通信业务的特点而提出的一种交换方式，将需要传送的数据按照一定的长度分割成许多小段数据，并在数据之前增加相应的用于对数据进行选路和校验等功能的头部字段，作为数据传送的基本单元，即分组。决定链路的方法有两种：无连接或面向连接。无连接在通信之前不需要建立连接，每个结点首先将前一个结点送来的分组收下，并保存在缓冲区中，然后根据分组头部中的地址信息选择适当的链路，将其发送至下一个结点；面向连接则是预先确定数据包的路径，每个数据包只需携带标识符，在帧中继中，这些标识符叫做数据链路连接标识符，交换机通过查询内存驻留表中的标识符确定前向路由。

由于交换机之间的内部链路由许多用户共享，因此，分组交换的成本低于电路交换。分组交换中的延迟（延时）和延时变化（抖动）大于电路交换网络。这是因为链路是共享的，数据包必须被某台交换机完全收到，才可继续传输到下一台交换机。尽管延时和抖动是共享网络与生俱来的特性，但现代技术可以在这些网络上实现令人满意的语音传输乃至视频通信。

14.1.4 广域网帧的封装格式***

广域网帧的封装格式有：

（1）点对点协议（Point-to-Point, PPP）：PPP 是一种标准协议，规定了同步或异步电路上的路由器对路由器、主机对网络的连接。当前 PPP 协议被广泛使用，本书下一章将专门讨论 PPP 协议。

（2）串行线路互连协议（Serial Line Internet Protocol, SLIP）：SLIP 是 PPP 的前身，用于使用 TCP/IP 的点对点串行连接。SLIP 基本上已经被 PPP 取代。

（3）高级数据链路控制协议（High level Data Link Control protocol, HDLC）：这里提到的 HDLC，是经过思科改装的 HDLC。HDLC 是点对点、专用链路和电路交换连接上默认的封装类型。HDLC 是按位访问的同步数据链路层协议，它定义了同步串行链路上使用帧标识和校验和的数据封装方法。当连接不同设备厂商的路由器时，要使用 PPP 封装（基于标准）。

(4) X.25: X.25 是帧中继的原型, 它指定 LAPB (Link Access Procedure Balanced, 平衡式链路访问程序) 为数据链路层协议。LAPB 是定义 DTE 与 DCE 之间如何连接的 ITU-T 标准, 是在公用数据网络上维护远程终端访问与计算机通信的。LAPB 用于包交换网络, 用来封装位于 X.25 中第 2 层的数据报。X.25 提供了扩展错误检测和滑动窗口的功能, 因为 X.25 是在错误率很高的模拟铜线电路上实现的。

(5) 帧中继 (Frame Relay): 帧中继指定 LAPF (Link Access Procedure Frame, 帧式链路访问程序) 为数据链路层协议。帧中继是一种高性能的包交换式广域网协议, 可以被应用于各种类型的网络接口中。X.25 用在错误率很高的模拟铜线电路上, 要执行错误检测; 帧中继用于高可靠性的数字传输设备上, 不执行错误检测, 错误检测由应用程序执行。帧中继比 X.25 的执行效率要高。

(6) ATM: ATM 是信元交换的国际标准, 在定长 (53 个字节) 的信元中能传输各种各样的服务类型 (如话音、音频、数据)。ATM 适于利用高速传输介质 (如 SONET)。



14.2 广域网技术**

本节讨论一些用于广域网连接的广域网技术, 包括模拟拨号、ISDN、租用线路、X.25、帧中继、ATM、DSL 和电缆调制解调器等, 并介绍各种广域网技术的优点、缺点和适用的环境。熟悉这些广域网接入在技术、速度和花费上存在差异很重要, CCNA 考试中会涉及给出场景, 要求选择适用的广域网技术。

14.2.1 广域网技术分类**

各种可供使用的广域网技术如图 14-2-1 所示。

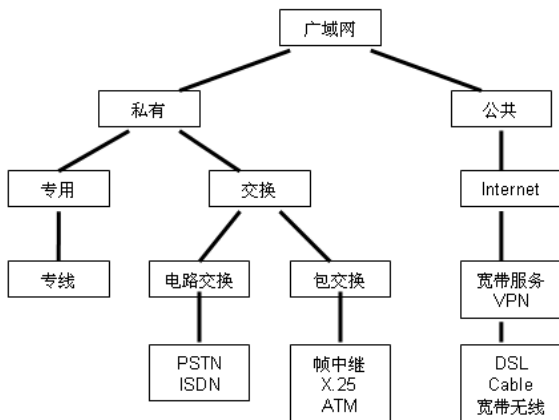


图 14-2-1 可供使用的广域网技术

1. 私有广域网

私有广域网包括专用线路和交换线路。交换线路又分为电路交换和包交换。

- 电路交换: 包括 PSTN (Public Switched Telephone Network, 公共交换电话网络, 稍后有介绍) 和 ISDN (Integrated Services Digital Network, 综合业务数字网, 稍后有介绍)。

- 包交换：包括帧中继、X.25 和 ATM。

2. 公共广域网

公共广域网连接使用互联网作为基础设施。直到现在，对一些广域网连接来说，Internet 仍然不是一种可行的选择，对很多企业来说，Internet 存在安全风险且缺乏足够的质量保障。通过使用 VPN 技术，互联网对性能要求不高的远程办公可以提供价格低廉和安全服务。公共广域网连接是通过宽带服务，如 DSL、电缆调制解调器、宽带无线，并结合 VPN 技术实现的。

14.2.2 广域网接入技术介绍*

1. PSTN

PSTN 是指常用的旧式电话系统，是一种全球语音通信电路交换网络，它也指简单的老式电话业务（POTS）。

电话网络是分布最广的通信网络，但传输的是模拟信号，需要经过调制解调器进行模数和数模的转换。它使用起来相对简单，而且对用户来说可以有很大的流动性和灵活性。通过电话网连接远程计算机特别适合家庭用户和出差人员与总部联络。

信号传输的速率受本地环路的物理特性限制，连接到 PSTN 的最高速率限制是 33Kb/s 左右。如果信号来自数字连接，速率可以增加至 56Kb/s 左右。如果再使用压缩技术，传输的速率还可以再快一些。

PSTN 连接的缺点是低速率和相对较长的连接时间，语音和视频流量无法在 PSTN 提供的低速链路上传输。

2. ISDN

综合业务数字网（Integrated Services Digital Network, ISDN）可经由现有的电话线路传输语音和数据资料。ISDN 与 PSTN 不同，PSTN 使用的是模拟线路，ISDN 使用的是纯数字线路。

ISDN 将本地环路转化为 TDM（Time Division Multiplex，时分多路复用）数字连接。该连接有用来传输语音或数据的 64Kb/s 承载（B）信道和一条用来进行呼叫建立及其他用途的信令（D）信道。

ISDN 目前主要提供两种类型服务：

- 基本速率接口（Basic Rate Interface, BRI）用于家庭和小型企业，提供 2 条 64Kb/s 的 B 信道和 1 条 16Kb/s 的 D 信道。整个链路速率可以达到 144Kb/s，可用于数据的有效传输是 128Kb/s。
- 基群速率接口（Primary Rate Interface, PRI）：用于大型企业。在北美和日本，PRI 提供 23B+1D，总速率达到 1.544Mb/s（包括用于同步的额外开销），称为 T1 速率。在欧洲、澳大利亚、中国和其他国家，PRI 提供 30B+1D，总速率达到 2.048Mb/s（包括用于同步的额外开销），称为 E1 速率。PRI 的 D 信道速率是 64Kbit/s。CCNA 考试中如果问到 PRI 的速率，要回答是 23B+1D，即 1.544Mb/s，毕竟 CCNA 是美国厂商的认证考试。

对于小型广域网，BRI 可以提供理想的连接机制。BRI 具有较短的呼叫建立时间（通常

小于 1 秒), 并且单一的 B 信道就可以提供比模拟调制解调器更快的速率, 如果需要更多的带宽, 第 2 条 B 信道也会被启用, 提供 128Kb/s 的速率。尽管这对于视频传输还不够, 但是它允许在传输数据时还可以同时有语音会话, 所以在 CCNA 考试中, 也认为 ISDN 可以支持语音、视频和数据。

ISDN 另外一个常见的应用是为专线提供冗余和备份, 当专线正常时, ISDN 可以分担一部分流量; 当专线故障时, ISDN 可以作为备份链路。

3. 专线

当需要永久专用连接时, 可以租用线路 (Leased lines), 也称专线, 专线可以提供多种不同的速率。专用线路的价格与线路的速率和两个连接点间的距离有关。专线一般比帧中继等共享的链路要贵。

每条租用线连接可以提供永久的专用容量, 提供有保障的服务。

但租用线连接也有缺点: 由于广域网的流量经常变化而租用线容量又是固定的, 这就造成带宽很少被完全使用。此外, 每条租用线连接都需要一个路由器的接口, 这使位于星型中心的路由器价格非常昂贵。

4. X.25

对应于专线的昂贵, Internet 服务提供商引入了分组交换网络中的共享线路来降低成本。第一个分组交换网络标准就是 X.25 协议族。

X.25 提供以下两种虚电路服务:

- 交换虚电路 (Switched Virtual Connection, SVC): 类似于电话交换, 即双方通信前要建立一条虚电路供数据传输, 通信完毕后要拆除这条虚电路, 供其他用户使用。
- 永久虚电路 (Permanent Virtual Connection, PVC): 可在两个用户之间建立永久的虚电路, 用户间需要通信时无须建立连接, 可直接进行数据传输, 像使用专线一样。由于 X.25 的计费不是基于连接时间和距离, 而是基于传输的数据量的, 所以它非常经济。

5. 帧中继

帧中继 (Frame Relay, FR) 是以 X.25 分组交换技术为基础, 摒弃其中复杂的检、纠错过程, 改造原有的帧结构, 从而获得了良好的性能。帧中继的用户接入速率一般为 64Kb/s~2Mb/s, 局间中继传输速率一般为 2Mb/s、34Mb/s, 现已可达 155Mb/s。

帧中继中的虚电路是为实现不同 DTE 之间的数据传输所建立的逻辑链路, 这种虚电路可以在帧中继交换网络内跨越任意多个 DCE 设备或帧中继交换机。虚电路为两个相互通信的 DTE 结点之间提供了面向连接的第 2 层服务。在帧中继网络中, 不同的虚电路由数据链路连接标识符 (Data-Link Connection Identifier, DLCI) 进行标识。

大多数的帧中继连接基于 PVC 而不是 SVC。帧中继的价格往往基于 CIR (Committed Information Rate, 承诺信息速率)。帧中继为承载语音和数据流量提供了永久的、共享的中等带宽的连接。帧中继是连接企业局域网的理想方式, 路由器可以只使用一个接口来提供多条 PVC。

一般来说, 帧中继技术适用于以下情况:

- 当用户需要数据通信时, 其带宽要求为 64Kb/s~2Mb/s, 而参与通信的各方多于两个时, 使用帧中继是一种较好的方案。

- 当数据业务量为突发性时，由于帧中继具有动态分配带宽的功能，选用帧中继可以有效地处理突发性数据。

本书第 16 章会介绍帧中继技术。

6. ATM

异步传输模式（Asynchronous Transfer Mode, ATM）可以提供更高带宽的低延迟和低抖动的永久共享式网络服务。ATM 技术综合了电路交换的可靠性与分组交换的高效性，借鉴了两种交换方式的优点，采用了基于信元的统计时分复用技术。

信元（Cell）是 ATM 用于传输信息的基本单元，其采用 53 个字节的固定长度。其中，前 5 个字节为信头，载有信元的地址信息和其他一些控制信息，后 48 个字节为信息段，装载来自各种不同业务的用户信息。固定长度的短信元可以充分利用信道的空闲带宽。信元在统计时分复用的时隙中出现，即不采用固定时隙，而是按需分配，只要时隙空闲，任何允许发送的单元都能占用。所有信元在底层采用面向连接方式传输，并对信元交换采用硬件以并行处理方式去实现，减少了结点的时延，其交换速度远远超过总线结构的交换机。

ATM 类似于其他共享式技术，如 X.25 和帧中继，它们的广域网结构看起来都一样，但 ATM 提供了更高流量水平的连接解决方案。ATM 非常适合传输语音和视频流量，因为信元是固定大小的 53 个字节，语音和视频流量不需要等待大数据分组的传输，延迟不会太长。

ATM 和帧中继一样，也提供 PVC 和 SVC，但广域网上一般使用 PVC，也允许在一条租用线路上有多条虚电路。

7. DSL

DSL 是目前世界上发展最快的高速宽带互联网接入技术，其全称是 Digital Subscriber Line（数字用户线路），包括 HDSL、SDSL、VDSL、ADSL 等，一般称之为 xDSL。它们的主要区别体现在信号传输速度和距离的不同，以及上行速率和下行速率对称性的不同这两个方面。其中 ADSL（Asymmetric Digital Subscriber Line，非对称数字用户线路）是目前世界上 xDSL 技术中应用最为广泛的一种。因为一般人上网通常是浏览网页寻找资料，而上传资料的量不是很多，ADSL 就是针对这样的网络使用特性，让计算机下载资料的速度高于上传资料的速度，所以被称为“非对称数字用户线路”。

DSL 的特点是以普通的铜质电话线为传输介质，实现广泛，并保护了原有投资。作为一种宽带网络连接技术，ADSL 的最快上传速率可达 1Mb/s，最快下行速率可达 8Mb/s，是普通 56Kb/s 调制解调器的 150 倍。另外，在使用 ADSL 时，由于语音和数据资料是分开传送的，上网不会影响电话的正常使用，使用 ADSL 上网并不需要缴付另外的电话费，且一直在线。

不同的 DSL 类型提供不同的带宽，大多数都超过了 T1 或 E1 租用线路。实际中所获得的速率主要取决于本地环路（也就是从用户到中心局）的实际长度和布线的类型与环境。为了能提供满意的服务，本地环路必须要小于 5.5 公里。

8. Cable Modem

电缆调制解调器，英文名称为 Cable Modem，它是近几年随着网络应用的扩大而发展起来的，主要借助于有线电视网进行数据传输。使用 Cable Modem，用户能够在接收有线电视服务的同时接收送往个人计算机的数据。Cable Modem 彻底解决了由于声音、图像的

传输而引起的阻塞，其速率已达 10Mb/s 以上，下行速率则更高。

Cable Modem 与以往的 Modem 在原理上都是将数据进行调制后在 Cable（电缆）的一个频率范围内传输，接收时进行解调，传输机理与普通 Modem 相同，不同之处在于它是通过有线电视 CATV（Community Antenna TV，共用天线电视，也就是有线电视网）的某个传输频带进行调制解调的。

使用 Cable Modem 的一个缺点是，所有本地用户共享电缆的带宽，就像使用同轴电缆的以太网连接的情况。当更多的用户使用这种服务时，实际的带宽可能比预期的要低。还有一个更加严重的缺点，那就是安全问题，由于 Cable Modem 所有用户的信号都是在同一根同轴电缆上进行传送的，因此有被搭线窃听的危险。

表 14-2-1 对各种广域网接入技术进行了对比。

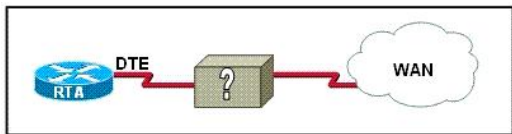
表 14-2-1 各种广域网接入技术

广域网接入技术	花 费	最大速度	连接类型	是否支持语音、视频和数据
专线	与距离和带宽有关	2.5Gb/s	永久、固定带宽	支持
PSTN	与距离和时间有关	56Kb/s	拨号低速连接	不支持
ISDN	与距离和带宽有关	128Kb/s	拨号中速连接	慢，但能凑合
X.25	按流量收费	48Kb/s	交换、固定带宽	不支持
帧中继	按带宽收费	4Mb/s	永久、固定带宽	支持
ATM	按带宽收费	155Mb/s	永久、固定带宽	支持
DSL	与时间和带宽有关	52Mb/s	各种 xDSL 技术	支持
Cable Modem	与时间和带宽有关	40Mb/s	共享	支持



14.3 真题精选***

1. Refer to the exhibit. The network administrator must complete the connection between the RTA of the XYZ Company and the service provider. To accomplish this task, which two devices could be installed at the customer site to provide a connection through the local loop to the central office of the provider? (Choose two.)



- WAN switch
 - PVC
 - ATM switch
 - multiplexer
 - CSU/DSU
 - modem
2. Which of the following describes the roles of devices in a WAN? (Choose three.)
- A CSU/DSU terminates a digital local loop.
 - A modem terminates a digital local loop.
 - A CSU/DSU terminates an analog local loop.
 - A modem terminates an analog local loop.
 - A router is commonly considered a DTE device.
 - A router is commonly considered a DCE device.

3. Which three Layer 2 encapsulation types would be used on a WAN rather than a LAN? (Choose three.)

- | | | |
|---------|-------------|----------------|
| A. HDLC | B. Ethernet | C. Token Ring |
| D. PPP | E. FDDI | F. Frame Relay |

4. At which layers of the OSI model do WANs operate? (Choose two.)

- | | | |
|----------------------|-------------------|--------------------|
| A. application layer | B. session layer | C. transport layer |
| D. network layer | E. datalink layer | F. physical layer |

5. When a router is connected to a Frame Relay WAN link using a serial DTE interface, how is the interface clock rate determined?

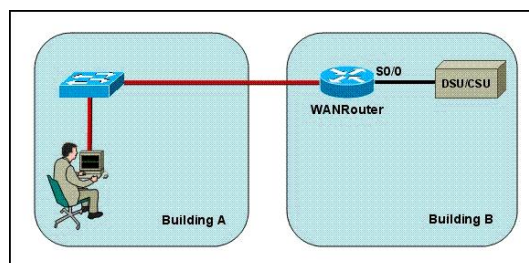
- A. It is supplied by the CSU/DSU.
- B. It is supplied by the far end router.
- C. It is determined by the clock rate command.
- D. It is supplied by the Layer 1 bit stream timing.

6. Refer to the exhibit. What is the reason that the interface status is "administratively down, line protocol down"?

```
Router# show interface s0/0/0
Serial 0/0/0 is administratively down, line protocol is down
```

- A. There is no encapsulation type configured.
- B. There is a mismatch in encapsulation types.
- C. The interface is not receiving any keepalives.
- D. The interface has been configured with the shutdown command.
- E. The interface needs to be configured as a DTE device.
- F. The wrong type of cable is connected to the interface.

7. Refer to the exhibit. The network administrator is in a campus building distant from Building B. WANRouter is hosting a newly installed WAN link on interface S0/0. The new link is not functioning and the administrator needs to determine if the correct cable has been attached to the S0/0 interface. How can the administrator accurately verify the correct cable type on S0/0 in the most efficient manner?



- A. Telnet to WANRouter and execute the command show interfaces S0/0
- B. Telnet to WANRouter and execute the command show processes S0/0
- C. Telnet to WANRouter and execute the command show running-configuration

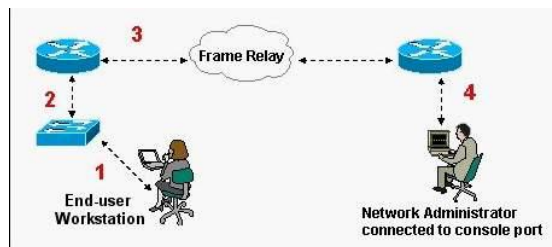
- D. Telnet to WANRouter and execute the command show controller S0/0
- E. Physically examine the cable between WANRouter S0/0 and the DCE.
- F. Establish a console session on WANRouter and execute the command show interfaces S0/0

8. The show interfaces serial 0/0 command resulted in the output shown in the graphic. What are possible causes for this interface status? (Choose three.)

```
Router# show interfaces serial 0/0
Serial0/0 is up, line protocol is down
Hardware is HD64570
Internet address is 192.168.100.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
```

- A. The interface is shut down.
- B. No keepalive messages are received.
- C. The clockrate is not set.
- D. No loopback address is set.
- E. No cable is attached to the interface.
- F. There is a mismatch in the encapsulation type.

9. Refer to the exhibit. What kind of cable should be used to make each connection that is identified by the numbers shown?

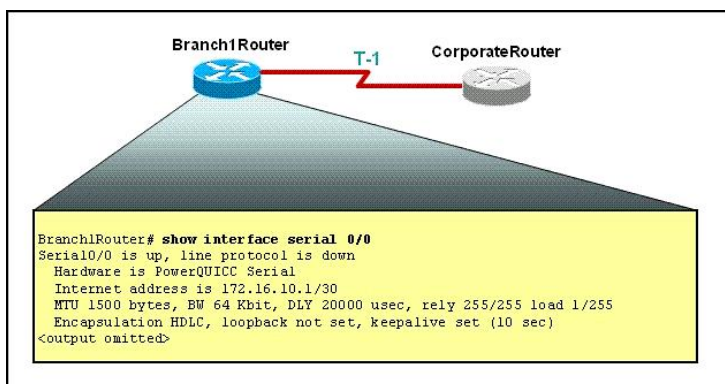


- | | |
|---|---|
| <ul style="list-style-type: none"> A. 1 - Ethernet crossover cable 2 - Ethernet straight-through cable 3 - fiber optic cable 4 - rollover cable | <ul style="list-style-type: none"> B. 1 - Ethernet straight-through cable 2 - Ethernet straight-through cable 3 - serial cable 4 - rollover cable |
| <ul style="list-style-type: none"> C. 1 - Ethernet rollover cable 2 - Ethernet crossover cable 3 - serial cable 4 - null modem cable | <ul style="list-style-type: none"> D. 1 - Ethernet straight-through cable 2 - Ethernet crossover cable 3 - serial cable 4 - rollover cable |
| <ul style="list-style-type: none"> E. 1 - Ethernet straight-through cable 2 - Ethernet crossover cable 3 - serial cable 4 - Ethernet straight-through cable | |

10. Refer to the exhibit. The corporate office and branch location have been attached

through two non-Cisco routers over a highly reliable WAN connection for over a year. A new Cisco router has been installed to replace the hardware at the branch location. Since the installation, IP communication cannot be verified across the link.

Given the output on Branch1Router, what would be a logical first step to take to resolve this problem?



- A. Change the encapsulation on CorporateRouter to HDLC.
- B. Verify successful DCE communication between the two sites.
- C. Change the encapsulation on Branch1Router to match CorporateRouter.
- D. Verify Layer 1 communication on the Branch1Router Serial 0/0 interface.
- E. Change the bandwidth setting on Branch1Router to match the actual line speed.
- F. Ensure an exact match between the bandwidth setting on CorporateRouter and Branch1Router.



14.4 真题解答***

1. 解：EF

题目问：参照图，网络管理员必须把 XYZ 公司的 RTA 路由器与服务提供商相连，为了完成这个任务，哪两个设备可以被安装在客户端来提供通过本地链路连接到提供商的中央办公室（选两个）？参照本章 14.1.2 节，如果是数字链路则使用 CSU/DSU；如果是模拟链路，则使用 Modem。

2. 解：ADE

题目问：下面哪一个描述了广域网中设备的角色（选三个）？参照本章 14.1.2 节的图 14-1-1，可知 ADE 正确。

3. 解：ADF

题目问：哪三个是广域网，而非局域网的二层封装（选三个）？连接到 WAN，有三种连接方式：专线连接、电路交换和包交换。专线使用同步串行线，它的二层的封装协议常用的有 HDLC、PPP；电路交换使用同步串行线，它使用的二层的封装协议有 HDLC、PPP；包交换使用的是虚电路（VC），而 VC 又分为 PVC（永久虚电路）和 SVC（交换虚电路），它使用的二层的封装协议有 X.25、Frame Relay、ATM。

4. 解: EF

题目问: 广域网工作在 OSI 模型的哪一层 (选两个)? WAN 是工作在一层和二层的。

5. 解: A

题目问: 当路由器使用一个串行的 DTE 接口连接到帧中继广域网链路时, 接口的时钟频率是如何决定的? 参照本章 14.1.2 节, 可知时钟频率是由 CSU/DSU 决定的。

6. 解: D

题目问: 参照图, 接口状态 “administratively down, line protocol down” 是什么原因? 这是一个非常简单的问题, D 正确。

7. 解: D

题目问: 网络管理员与建筑物 B 相距很远, WANRouter 路由器的 S0/0 接口刚被接入广域网, 新接的链路不能工作, 管理员想检查 S0/0 接口是否被连接了正确的线缆, 管理员怎样以最高效的方式验证 S0/0 接口有没有使用正确的线缆? 要检验接口 S0/0 的线缆类型, 首先要登录到路由器上去, 可以通过 Telnet 的技术登录上去, 查看接口所接的线缆的类型使用的命令为 “show controller s0/0”, 可以看到接口连接的线缆类型, 以及是 DTE 还是 DCE 端。本章 14.1.2 节介绍了这个命令的使用。

8. 解: BCF

题目问: 图中显示了 “show interfaces serial 0/0” 命令的输出, 可能是什么原因导致接口出现这种状态? 接口封装类型不一致, 没有配置时钟, 以及没有收到激活消息都会导致接口的协议 Down。如果被人为关闭, 出现的提示是 “administratively down, line protocol Down”; 如果没有连接线缆, 出现的提示是 “Serial 0/0 is down, line protocol down”。物理接口的状态与有没有配置环回接口无关。

9. 解: B

题目问: 参照图, 图中标出的每一个数字部分将使用什么类型的线缆? 计算机与交换机、路由器与交换机都属于不同类型的设备, 使用直通的双绞线; 路由器与帧中继网络相连, 使用的是串行接口, 当然要使用串行线; 要通过 Console 口对路由器进行配置, 需使用配置线, 配置线是全反线。

10. 解: C

题目问: 参照图, 中心办公室和分支办公室通过两台非思科的路由器相连, 已经正常工作超过了一年, 一个新的思科路由器被安装来替换分支机构的路由器, 自从安装新的路由器后, IP 通信失败。图中给出了分支路由器的输出, 为了解决这个问题, 逻辑上第一步应该做什么? 注意到思科路由器串行接口的默认封装是 HDLC, 思科使用的 HDLC 是经过改装的私有 HDLC, 虽然说思科允许其他厂家使用它私有的 HDLC, 但其他厂家的路由器并不一定使用这种封装协议, 题中也提到了原来的两台路由器都不是思科路由器, 所以它们使用的封装协议不好确定。选项 A 说改变中心站点的路由器使用 HDLC 封装, 则不一定能成功, 首先中心站点的路由器是否支持 HDLC 封装, 它所使用的 HDLC 是否是思科私有的 HDLC。C 选项则更合理, 把分支路由器的封装改成与中心站点匹配的封装。

第 15 章

PPP**

PPP (Point-to-Point Protocol, 点到点协议) 支持在各种物理类型的点到点串行线路上传输上层协议报文。PPP 有很多丰富的可选特性, 如支持多协议、提供可选的身份认证服务、支持多种方式压缩数据、支持动态地址分配、支持多链路捆绑等, 这些丰富的特性增强了 PPP 的功能。同时, 不论是异步拨号线路还是路由器之间的同步链路均可使用 PPP 封装, 应用十分广泛。

本章将对 PPP 的上述特性进行介绍, 演示相关功能的配置, 重点介绍 PPP 的两种验证方式。



15.1 PPP 概述**

本节介绍 HDLC 协议、同步和异步串行通信、PPP 协议的特点、PPP 协议的分层体系结构、PPP 会话的建立过程等。

15.1.1 HDLC**

HDLC 是思科路由器串行接口的默认封装协议。串行接口是与并行接口相对而言的, 计算机有串口也有并口。比如使用 RS-232 连接计算机的 COM 口 (9 针) 和路由器的 Console 口, 使用的就是串行通信, 在串行通信中, 数据按 Bit 传输, 即一次传输一个比特。计算机上还有一种并口 (25 针), 经常被用来连接老式打印机, 并行通信中数据按 Byte 传输, 即一次传输一个字节, 8 个比特, 速度是串行通信的 8 倍。并行通信虽然速度较快, 但因为线缆较贵, 内部的多根线缆同步也较困难, 且相互间易产生干扰, 所以在远距离的通信中大多使用串行通信, 在计算机内部大多使用并行通信。

标准的 HDLC 封装只能支持单协议, 即 IP 协议, 思科对标准的 HDLC 协议进行了改进, 增加了协议域字段, 来支持多种网络层协议。虽然说改进的 HDLC 是思科的私有协议, 但思科也允许其他网络设备制造商使用改进的 HDLC 协议。

在 Packet Tracer 模拟器中拖出自定义的思科 1841 路由器, 或者拖出一台标准的思科 1841 路由器, 并添加串行接口模块。使用 “show interfaces serial 0/1/0” 命令查看路由器串行接口的封装协议, 显示如下:

```
Router#show interfaces serial 0/1/0
Serial0/1/0 is administratively down, line protocol is down (disabled)
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

从上面的输出中可以看到, 在 Cisco 路由器串行接口上的默认封装协议是 HDLC。思科

路由器上之所以默认使用 HDLC 封装,是因为路由器之间用同步串行接口连接时,采用 Cisco HDLC 比采用 PPP 协议效率要高得多。但是,如果将 Cisco 路由器与非 Cisco 路由器进行同步专线连接时,最好不要使用 HDLC,因为思科的 HDLC 是私有的,其他厂家的设备不一定支持思科私有的 HDLC 协议,可以采用 PPP 协议。

如果接口的封装协议不是 HDLC,可以使用下面的命令把串行接口的封装协议更改成 HDLC:

```
Router(config)#int s0/1/0
Router(config-if)#encapsulation hdlc
```

15.1.2 同步和异步串行通信*

串行通信又分为同步传输和异步传输。

1. 异步传输

通常,异步传输是以字符为传输单位的,每个字符都要附加 1 位起始位和 1 位停止位,以标记一个字符的开始和结束,并以此实现数据传输同步。所谓异步传输,是指字符与字符(一个字符结束到下一个字符开始)之间的时间间隔是可变的,并不需要严格地限制它们的时间关系。

异步传输又称为起止式异步通信方式,其优点是简单、可靠,适用于面向字符的、低速的异步通信场合。例如,计算机与 Modem 之间的通信就是采用这种方式。它的缺点是通信开销大,每传输一个字符都要额外附加 2~3 位,通信效率比较低。

说得直观点,异步传输是指:发送方发出数据后,不等接收方发回响应,接着发送下个数据包的通信方式,这非常适合拨号这种慢速的连接方式。

2. 同步传输

通常,同步传输是以数据块为传输单位。每个数据块的头部和尾部都要附加一个特殊的字符或比特序列,标记一个数据块的开始和结束,一般还要附加一个校验序列(如 16 位或 32 位 CRC 校验码),以便对数据块进行差错控制。所谓同步传输,是指数据块与数据块之间的时间间隔是固定的,必须严格地规定它们的时间关系。

说得直观点,同步传输是指:发送方发出数据后,等接收方发回响应以后才发下一个数据包的通信方式。路由器串行接口属于快速的同步接口,进行的是同步传输,需要在 DCE 端配置时钟,来进行信号同步。

如果读者还是不太明白同步和异步的区别,看下面的比喻。

同步就是你我说话,我每听到一句话都应答一声,你听到我的应答后,继续说下一句;如果你没有收到我的应答,就重复最后说的那句话,直到收到了我的应答,才继续说下一句。

异步就是你我说话,不用等到我的应答,你可以继续说下面的那句话。

15.1.3 PPP 特点**

PPP 是 IETF 推出的点到点类型线路的数据链路层封装协议,它解决了 SLIP 和 HDLC 中的问题,并成为正式的因特网标准。

PPP 协议被仔细地设计用来和大多数的硬件保持兼容。PPP 支持多种物理链路,可以在以下类型的物理接口上配置 PPP:

- 同步串行接口
- 异步串行接口
- 高速串行接口 (HSSI)
- 综合业务数字网 (ISDN)

此外, 现在 PPP 还被广泛地使用在以太网和 ATM 上, 称为 PPPoE (PPP over Ethernet) 和 PPPoA (PPP over ATM)。

PPP 提供了一些 HDLC 所不具备的功能, 如支持 IP 地址动态分配、链路质量检测、多链路捆绑、多种压缩、PAP 或 CHAP (后面会介绍到这两种验证方式) 验证等。

PPP 利用三个主要的组件来解决网际网络连接的问题:

- 在点对点链路上使用高级数据链路控制 (HDLC) 封装数据。PPP 帧格式以 HDLC 帧格式为基础, 做了很少的改动。
- 使用 LCP (Link Control Protocol, 链路控制协议) 来建立、设定和测试数据链路连接。
- 使用 NCPs (Network Control Protocols, 网络控制协议系列) 建立和设定不同的网络层协议。PPP 的设计是为了同时使用多种网络层协议。今日, PPP 能支持 IP 以外的其他协议, 包括 Novell IPX、AppleTalk 等。PPP 使用其 NCP 组件来封装多重协议。

15.1.4 PPP 分层体系结构***

分层体系架构是一个逻辑模型, 图 15-1-1 把 PPP 的分层体系结构和 OSI 参考模型进行了对比, PPP 和 OSI 共享相同的物理层, PPP 分为 LCP 和 NCP 功能子层, LCP 包含在 OSI 参考模型的数据链路层内, 而 NCP 跨越 OSI 参考模型的数据链路层和网络层。

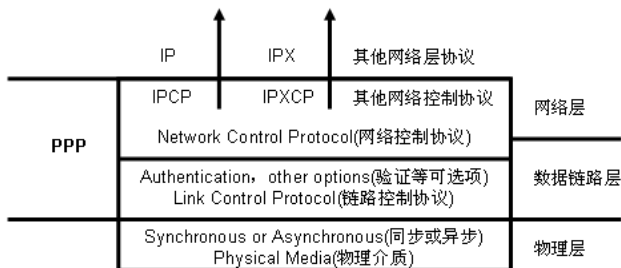


图 15-1-1 PPP 的层次结构

PPP 支持各种类型的硬件, 包括 EIA/TIA232、EIA/TIA449、EIA/TIA530、V.35、V.21 等, 只要是点到点类型的线路都可以运行 PPP。在数据链路层, PPP 通过 LCP 协议进行链路管理, 相当于以太网数据链路层的 MAC 子层。而在网络层, 由 NCP 为不同的协议提供服务。这里的 NCP 相当于以太网数据链路层的 LLC 子层。

1. LCP 子层

LCP 位于物理层之上, 除了用来建立、配置和测试数据链路连接外, 还提供下列可选的功能选项。

(1) **身份验证 (Authentication)**。路由器间相互验证身份, 验证的方法有 PAP 和 CHAP。

(2) **压缩 (Compression)**。PPP 协议运行在速率十分有限的点到点串行链路上。为了提高数据发送效率, 可以采用对数据进行压缩后再传送的方法, 称为链路压缩。通过减少链

路中数据帧所含数据的大小，来提高 PPP 线路的吞吐量。但压缩和解压缩会增加两端路由器的负担，也会带来压缩和解压缩延时。

LCP 支持以下一些链路压缩方法：Stac、Predictor、MPPC，以及 TCP 头部压缩。不同的方法对 CPU 及内存的需求并不相同，有些需要更多的内存（内存密集型），有些则需要占用更多的 CPU 时间（CPU 密集型）。压缩原理和效果也不相同。

- **Stac**: Stac 压缩算法基于 Lempel-Ziv 理论，它通过查找、替换传送内容中的重复字符串的方法达到压缩数据的目的。使用 Stac 压缩算法可以选择由各种硬件（适配器、模块等）压缩或者由软件进行压缩，还可以选择压缩的比率。Stac 压缩算法需要占用较多的 CPU 时间。
- **MPPC**: MPPC 是微软的压缩算法实现，它也是基于 Lempel-Ziv 理论，也需要占用较多的 CPU 时间。
- **Predictor**: Predictor 即预测算法通过检查数据的压缩状态（是否已被压缩过）来决定是否进行压缩。因为，对数据的二次压缩一般不会有更大的压缩率。相反，有时经过二次压缩的数据反而比一次压缩后的数据更大。Predictor 算法需要占用更多的内存。
- **TCP 头部压缩**: 通过删除 TCP 头部一些不必要的字节来实现数据压缩的目的。

(3) **错误检测 (Error Detection)**。PPP 的错误检测机制使进程能够识别错误的情形。Quality 选项用来监视链路质量。

(4) **多链路 (Multilink)**。多链路捆绑，在一条链路负载达到一定数值的情况下，启用第二条链路。多条链路间可以实现负载均衡。

(5) **PPP 回拨 (PPP callback)**。它被用来进一步提高安全性和节省费用或统一支出费用。客户发起一个初始呼叫，请求回拨，并且终止初始的呼叫。回拨路由器依照配置语句回应初始呼叫，并向客户回拨。这样拨号的费用统一由服务端支付，假如服务端可以享受话费方面的优惠，这样回拨将是一种经济的方法。另外，假如有攻击者尝试发动攻击，服务端拒绝呼叫，并主动呼叫配置中的号码，攻击者的直接攻击将失败，这可以进一步提高安全性。

2. NCP 子层

当 LCP 将链路建立好了以后，PPP 开始根据不同用户的需要，配置上层协议所需的环境。PPP 使用网络控制协议 (NCP) 来为上层提供服务接口。针对上层不同的协议类型，会使用不同的 NCP 组件。比如对于 IP 提供 IPCP 接口，对于 IPX 提供 IPXCP 接口，对于 AppleTalk 提供 ATCP 接口等。

15.1.5 PPP 会话建立过程*

PPP 提供了建立、配置、维护和终止点到点连接的方法。从开始发起呼叫到最终通信完成后释放链路，PPP 的工作经历了 4 个阶段。

阶段 1，链路的建立和配置协商。这主要是 LCP 的功能，通信的发起方发送 LCP 帧来配置和检测数据链路。

阶段 2，链路质量检测 (可选阶段)。这属于 LCP 层的可选功能，主要是测试链路的质量能否满足要求。如果链路质量不能满足要求，则建立链路失败。

阶段 3，网络层协议的配置阶段。这主要是 NCP 的功能，通信双方开始交换一系列的 NCP 分组来配置网络层。对于上层使用的是 IP 协议的情形来说，此过程是由 IPCP 完成的。

当 NCP 配置完成后, 双方的逻辑通信链路就建立好了, 双方可以开始在此链路上交换上层数据。任何阶段的协商失败都将导致链路的拆除。

阶段 4, 链路终止。当数据传送完成后或一些外部事件发生(如空闲时间超长或用户干预)时, 一方会发起断开连接的请求。这时, 首先使用 NCP 来释放网络层的连接, 然后利用 LCP 来关闭数据链路层的连接; 最后, 双方的通信设备或模块关闭物理链路回到空闲状态。

15.1.6 PPP 身份验证协议***

PPP 身份验证功能是可选的。如果启用了验证功能, 验证过程将发生在网络层协议配置阶段开始之前。身份验证功能需要呼叫的发起方输入验证信息, 这个信息用来确定用户拥有对应的呼叫许可。对等路由器之间相互交换身份验证信息。PPP 有两种可供选择的身份验证方式: PAP 和 CHAP。

1. PAP

PAP (Password Authentication Protocol, 密码验证协议) 是一种两次握手验证协议, 它在网络上采用明文方式传输用户名和口令。PAP 验证如图 15-1-2 所示, 验证的过程如下:

(1) 被验证方主动发起验证请求, 将本端的用户名和口令发送到验证方。

(2) 验证方接到被验证方的验证请求后, 检查此用户名是否存在, 以及口令是否正确。如果此用户名存在且口令正确, 验证方返回接受报文, 表示验证通过; 如果此用户名不存在或口令错误。验证方返回拒绝报文, 表示验证不通过。

从图 15-1-2 中可以看出, R1 是被验证路由器, R2 是验证路由器, R2 上配置了用户名 cisco, 对应的密码也是 cisco。R1 想连接到 R2, R1 发送 cisco cisco 的用户名和密码, R2 如果在数据库中检测到, 则接受 R1 的连接请求; 如果找不到对应的用户名和密码, 则拒绝 R1 的连接请求。

从 PAP 验证的过程可以看出, PAP 不是一种健壮的身份验证协议。首先, 密码在链路上是明文传输的, 极易被捕获而造成泄密; 其次, 由于验证重试的频率和次数由被验证方控制, 因此不能防止回放攻击和重复的尝试攻击, 被验证方可以运行一些暴力破解软件, 破解密码只是早晚的事。

2. CHAP

CHAP (Challenge Handshake Authentication Protocol, 挑战握手验证协议) 是一种三次握手验证协议, 它只在网络上传输用户名, 而用户口令并不在网络上传播。CHAP 作用在 LCP 初始链路建立之后, 而且在链路建立成功后任何时间都可以进行重复验证。CHAP 验证如图 15-1-3 所示。

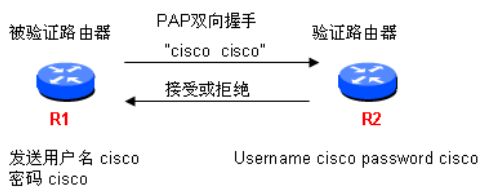


图 15-1-2 PAP 验证

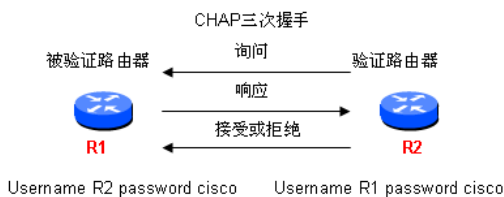


图 15-1-3 CHAP 验证

CHAP 验证过程如下:

(1) 在 PPP 链路建立阶段完成之后, 验证方主动发起验证挑战 “Challenge”, 向被验证方发送一些随机产生的报文, 并同时将被验证方的主机名附带上一起发送给被验证方。如图 15-1-4 所示, R1 拨入 R2, R2 发出挑战报文。“01” 是序号; R2 上可能会有多个拨入请求, “id” 用来识别是向哪个拨入者发出的挑战; “random” 是一个随机数; “R2” 是发起挑战路由器的名字。

(2) 被验证方接到验证方的验证请求后, 根据此报文中的主机名在本路由器的数据库中查找用户名和口令。如果找到相同的用户名, 便利用报文 id 和此用户名对应的口令, 以及发过来的随机数, 以 MD5 算法生成一个 Hash 值。如图 15-1-5 所示, 路由器 R1 根据 R2 发送过来的挑战报文计算 Hash 值。

被验证方将验证方发过来的 id 值和生成的 Hash 值, 以及本路由器的名字发回。如图 15-1-6 所示, “02” 是序号; “id” 是验证服务器发过来的序号, 用来区分可能存在的多个拨入者; Hash 值是前面计算出来的; “R1” 是被验证路由器的名字。

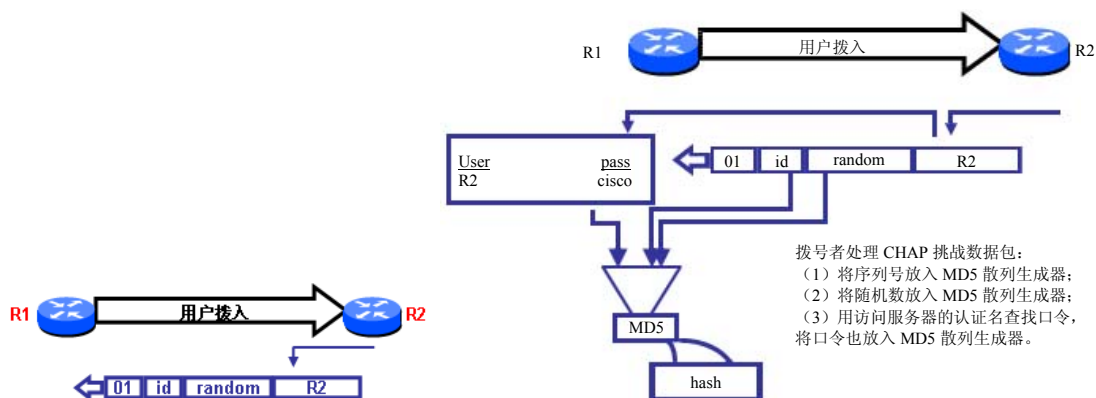


图 15-1-5 CHAP 验证第二步: 被验证方计算 Hash 值

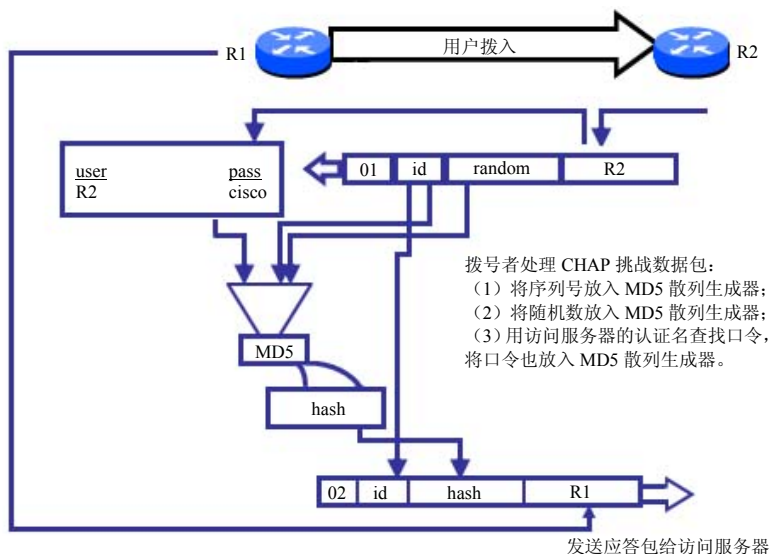


图 15-1-6 CHAP 验证第二步: 被验证方发送应答包给访问服务器

读者可以注意到,在步骤 2 中并没有发送明文的密码,而是发送了一个由密码、随机数和 id 值共同计算出来的一个 Hash 值。由于 Hash 算法的不可逆性,很难从 Hash 值推导出来使用的密码。

(3) 验证方接收到此应答后,利用报文 id 找到本地保存的随机数,并根据发过来的被验证路由器的名字在数据库中查找用户名对应的密码,然后用 id、随机数和密码,经 MD5 算法得出一个 Hash 值,与被验证方发过来的 Hash 值进行比较,如图 15-1-7 所示。

如果两者相同,则返回接受报文,如图 15-1-8 所示,序号“03”表示验证通过。如果两者不相同,则返回拒绝报文,表示验证不通过,序号是“04”。

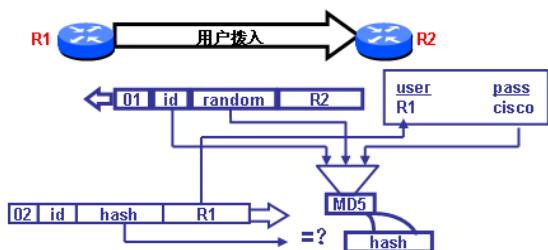


图 15-1-7 CHAP 验证第三步：比较 Hash 值

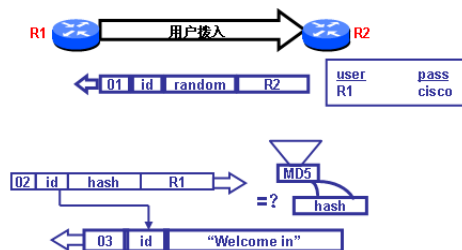


图 15-1-8 CHAP 验证第三步：验证通过



15.2 配置 PPP**

本节介绍 PPP 基本配置、PAP 和 CHAP 验证配置。

15.2.1 PPP 基本配置**

1. 配置 PPP 封装

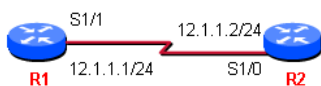


图 15-2-1 PPP 封装

对于同步串行接口,默认的封装格式是 HDLC。可以使用“encapsulation ppp”命令将封装格式改为 PPP。本节的实验使用 Dynamips 的 CCNA 机架,R1 和 R2 的连接如图 15-2-1 所示。

路由器 R1 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
```

路由器 R2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
```

在 R1 上测试到 R2 的连通性,显示如下:

```
R1#ping 12.1.1.2
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 12.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/15/24 ms
```

从上面的输出中可以看出，R1 可以 ping 通 R2。

查看 R1 接口的封装，显示如下：

```
R1#show int s1/1
Serial1/1 is up, line protocol is up
  Hardware is M4T
  Internet address is 12.1.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
```

可以看出 R1 接口的默认封装协议是 HDLC。使用同样的方法，也可以得知 R2 的 S1/0 接口封装的也是 HDLC 协议。使用下面的命令把 R1 的 S1/1 接口的封装协议改成 PPP：

```
R1(config)#int s1/1
R1(config-if)#encapsulation ppp
```

当在 R1 的 S1/1 接口配置完 PPP 封装后，R1 的控制台显示提示信息 “*Jul 29 23:35:16.599: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1, changed state to down”，类似的信息在 R2 的控制台也有显示。

当通信双方的某一方封装格式为 HDLC，而另一方为 PPP 时，双方关于封装协议的协商将失败。此时，此链路处于协议关闭状态，通信无法进行。使用 “show ip int brief” 命令，查看路由器 R1 接口的 IP 状态，显示如下：

```
R1#show ip int brief
Interface      IP-Address      OK? Method Status        Protocol
FastEthernet0/0 unassigned      YES unset  administratively down down
Serial1/0      unassigned      YES unset  administratively down down
Serial1/1      12.1.1.1        YES manual up            down
Serial1/2      unassigned      YES unset  administratively down down
Serial1/3      unassigned      YES unset  administratively down down
FastEthernet2/0 unassigned      YES unset  administratively down down
```

在路由器 R1 上 ping R2 的 IP 地址，通信失败。

使用下面的命令把 R2 的 S1/0 接口的封装协议也改成 PPP：

```
R2(config)#int s1/0
R2(config-if)#encapsulation ppp
```

稍后 R2 的控制台显示 “*Jul 29 23:41:17.619: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up”，提示 S1/0 接口的协议正常了，R1 上显示类似的信息。

测试 R1 和 R2 之间的连通性，通信成功。查看 R1 的 S1/1 接口的封装，显示如下：

```
R1#show int s1/1
Serial1/1 is up, line protocol is up
  Hardware is M4T
  Internet address is 12.1.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, crc 16, loopback not set
```

注意到 R1 的 S1/1 接口的封装协议已经改成了 PPP，LCP Open 表示链路协商成功，Open:IPCP 表示 NCP 也建立成功。

2. 配置压缩

使用压缩会影响路由器的性能，如果要传送文件已经由压缩文件组成，比如 ZIP、RAR、

MPEG 等，则不要使用压缩选项。

配置压缩的命令如下：

```
R1(config)#int s1/1
R1(config-if)#compress ?      显示压缩的类型。
  lzs      lzs compression type
  mppc     MPPC compression type
  predictor predictor compression type
  stac     stac compression algorithm
  <cr>
R1(config-if)#compress predictor 使用 predictor 压缩。
```

同样，配置 R2 的 S1/0 接口的压缩。

3. 配置链路质量监控（Link Quality Monitoring, LQM）

本章 15.1.5 节“PPP 会话建立过程”的阶段 2，提到了一个可选的阶段链路质量检测。在这个阶段，LCP 测试链路并决定链路的质量能否满足第三层协议的需要，如果链路质量不能满足要求，链路将被关闭。使用的命令是“ppp quality percentage”（百分比），计算数据包发送和接收的成功率。如果链路质量百分比不能达到要求，则认为链路质量太差，断开连接。配置链路质量百分比的命令如下：

```
R1(config)#int s1/1
R1(config-if)#ppp quality 80      链路有效要大于 80%，否则认为链路无效。
```

4. 配置链路负载均衡

Multilink PPP（多链路 PPP，有时也称 MP、MPPP、MLP 或 Multilink）允许包被分段，在到对方的多条点对点上同时被发送。配置的命令如下：

```
R1(config)#int s1/1
R1(config-if)#ppp multilink
```

15.2.2 PPP 验证配置***

1. PPP 验证过程

PPP 的验证过程如图 15-2-2 所示，如果进入的 PPP 协商报文不要求验证，则开始后面的 PPP 处理过程；如果要求验证，则使用的验证数据库可能是路由器本地的数据库，也可能是专门的验证服务器，比如 AAA（Authentication、Authorization 和 Accounting，认证、授权和记账）服务器，AAA 属于 CCNP 的内容。如果验证成功，则开始后面的 PPP 处理过程；如果验证失败，则断开连接。

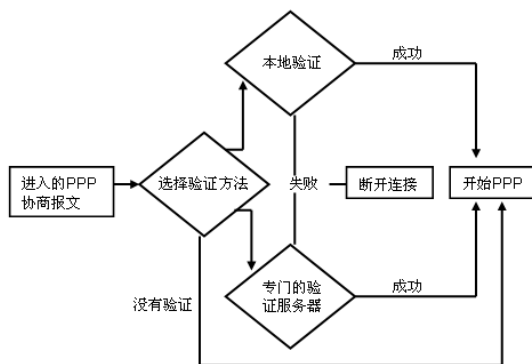


图 15-2-2 PPP 的验证过程

2. PAP 验证

配置图 15-2-1 中的两台路由器使用 PPP 封装。路由器 R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)# encapsulation ppp
```

路由器 R2 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R1(config-if)# encapsulation ppp
```

接下来配置 PAP 验证，R1 的配置和说明如下：

```
R1(config)#username R2 password cisco2      配置本地验证使用的用户名和密码。
R1(config)#int s1/1
R1(config-if)#ppp authentication pap        选择 PPP 的验证方式。
R1(config-if)#ppp pap sent-username R1 password cisco1
配置要发送 PAP 验证的用户名和密码到远端路由器。因为 CHAP 验证是一种更安全的验证方式，在默认情况下，
路由器不会发送 PAP 的用户名和密码，需要使用这条命令强制发送 PAP 的用户名和密码。远端路由器上有
“username R1 password cisco1”的配置语句。既然是可以手工指定发送路由器名，这里也可以换成“ppp
pap sent-username test password cisco1”，只要 R2 上有“username test password cisco1”，
验证就可以通过。
```

R2 的配置和说明如下：

```
R2(config)#username R1 password cisco1      这里的配置要与 R1 的 S1/1 接口发送过来的用户名
和 密码对应。
R2(config)#int s1/0
R2(config-if)# ppp authentication pap
R2(config-if)#ppp pap sent-username R2 password cisco2      这里的配置也是与 R1 的 “username
R2 password cisco2” 相呼应。
```

配置完成后，测试 R1 和 R2 之间的连通性，可以正常通信。

从上面的配置中，可以得出三点结论：一、PAP 并不是路由器推荐的验证方式，需要在接口下强制发送 PAP 的验证信息；二、PAP 验证中的用户名并不一定非要是对方路由器的名字；三、两端路由器可以配置不一样的密码。

3. CHAP 验证

首先取消路由器 R1 和 R2 上的 PAP 验证配置。R1 的操作如下：

```
R1(config)#no username R2
R1(config)#int s1/1
R1(config-if)#no ppp pap sent-username
R1(config-if)#no ppp authentication
```

R2 的操作如下：

```
R2(config)#no username R1
R2(config)#int s1/0
R2(config-if)#no ppp pap sent-username
R2(config-if)#no ppp authentication
```

接下来配置 CHAP 验证，R1 的配置和说明如下：

```
R1(config)#username R2 password cisco
```

配置本地验证使用的用户名和密码，这里的用户名要使用对方路由器的名字。本章 15.1.6 节中介绍到，要根据对端路由器的名字在验证数据库中查找密码。

```
R1(config-if)#ppp authentication chap
```

配置 CHAP 验证，CHAP 验证是路由器推荐的验证方式，所以不用像 PAP 验证那样，还要配置发送的用户名和密码。

R2 的配置和说明如下：

```
R2(config)#username R1 password cisco
```

同理，这里的用户名要使用远端路由器的主机名。在 CHAP 验证中，两端配置的密码一定要相同，从本章 15.1.6 节中可以得知，两端的路由器要基于密码计算 Hash 值，如果两端的密码不同，计算出来的 Hash 值就不相同，将会导致验证失败，这一点与 PAP 验证不同。

```
R2(config-if)#ppp authentication chap
```

这里要提醒读者的是，CHAP 验证是随机的，因为当前链路已经 UP，即使 CHAP 验证是失败的也不会马上表现出来。最好的测试办法是关闭路由器的物理接口，再打开路由器的物理接口，强制 CHAP 在链路刚建立时进行验证。

```
R1(config)#int s1/1
R1(config-if)#shut
*Mar 1 00:49:16.451: %LINK-5-CHANGED: Interface Serial1/1, changed state to
administratively down
*Mar 1 00:49:17.451: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1, changed
state to down
R1(config-if)#no shut
*Mar 1 00:50:24.879: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
*Mar 1 00:50:25.959: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1, changed
state to up
```

配置完成后，测试 R1 和 R2 之间的连通性，可以正常通信。

从上面的配置中，可以得出两点结论：一、CHAP 验证中的用户名要是对方路由器的主机名；二、两端路由器使用的密码要相同。

4. PPP 验证的排错

可以使用“debug ppp authentication”命令查看 PPP 的验证情况。在路由器 R2 上使用“debug ppp authentication”命令，发现并没有信息输出，这是因为 CHAP 验证是随机的。关闭 R2 的 S1/0 接口，稍后再打开，输出的信息显示如下：

```
*Jul 30 23:04:23.019: Se1/0 PPP: Authorization required
*Jul 30 23:04:23.031: Se1/0 CHAP: O CHALLENGE id 66 len 23 from "R2"
*Jul 30 23:04:23.043: Se1/0 CHAP: I CHALLENGE id 64 len 23 from "R1"
*Jul 30 23:04:23.047: Se1/0 CHAP: Using hostname from unknown source
*Jul 30 23:04:23.047: Se1/0 CHAP: Using password from AAA
*Jul 30 23:04:23.047: Se1/0 CHAP: O RESPONSE id 64 len 23 from "R2"
*Jul 30 23:04:23.051: Se1/0 CHAP: I RESPONSE id 66 len 23 from "R1"
*Jul 30 23:04:23.063: Se1/0 PPP: Sent CHAP LOGIN Request
*Jul 30 23:04:23.071: Se1/0 PPP: Received LOGIN Response PASS
*Jul 30 23:04:23.071: Se1/0 PPP: Sent LCP AUTHOR Request
*Jul 30 23:04:23.071: Se1/0 PPP: Sent IPCP AUTHOR Request
*Jul 30 23:04:23.075: Se1/0 LCP: Received AAA AUTHOR Response PASS
*Jul 30 23:04:23.079: Se1/0 IPCP: Received AAA AUTHOR Response PASS
*Jul 30 23:04:23.079: Se1/0 CHAP: O SUCCESS id 66 len 4
*Jul 30 23:04:23.083: Se1/0 CHAP: I SUCCESS id 64 len 4
*Jul 30 23:04:23.091: Se1/0 PPP: Sent CDPCP AUTHOR Request
*Jul 30 23:04:23.099: Se1/0 CDPCP: Received AAA AUTHOR Response PASS
*Jul 30 23:04:23.111: Se1/0 PPP: Sent IPCP AUTHOR Request
```

从上面的输出中可以看到，目前使用的是双向验证，“O”指的是 out（外出）方向的验证，“I”指的是 input（进入）方向的验证，最后进出方向的验证均成功（SUCCESS）。

5. PPP 验证的选项

PPP 除了上面单独配置的 PAP 或 CHAP 验证外，还可以同时使用两种验证。如“ppp

authentication pap chap”，同时使用 PAP 验证和 CHAP 验证，优选 PAP 验证。

PPP 验证还可以是单向验证，使用的命令是“ppp authentication 验证方式 callin”，只对呼入使用验证。



15.3 真题精选***

1. Which of the following are key characteristics of PPP? (Choose three)

- A. can be used over analog circuits
- B. maps Layer 2 to Layer 3 address
- C. encapsulates several routed protocols
- D. supports IP only
- E. provides error correction

2. What can a network administrator utilize by using PPP Layer 2 encapsulation?

(Choose three)

- | | |
|----------------------|-----------------------|
| A. VLAN support | B. compression |
| C. authentication | D. sliding windows |
| E. multilink support | F. quality of service |



15.4 真题解答***

1. 解：ACE

题目问：下面哪一个是 PPP 的关键特点（选三个）？PPP 支持的链路有同步、异步串行线路、ATM（PPPoA）、以太网（PPPoE）、电话线路（模拟线路）等；PPP 使用 NCP 子层来支持多种网络层协议，包括 IP、IPX、AppleTalk 等；PPP 使用 LCP 子层来支持身份验证、链路质量检测、多链路捆绑、回拨和压缩等。

2. 解：BCE

题目问：管理员可以利用 PPP 二层封装的哪些方面（选三个）？本题实际上也是问 PPP 的优点，从第 1 题的解释中，可以得知 BCE 是正确答案。

第 16 章

帧中继***

本章将从帧中继的由来讲起，介绍帧中继术语、帧中继运行方式、帧中继本地管理接口、帧中继全局寻址、帧中继子接口，并演示帧中继配置。



16.1 帧中继概述***

帧中继是 20 世纪 80 年代初发展起来的一种数据通信技术，其英文名为 Frame Relay，简称 FR。本节主要介绍帧中继的相关术语和概念。

16.1.1 帧中继优点*

帧中继可以看做是 X.25 协议的简化版本，帧中继在操作处理上做了大量的简化。帧中继不考虑传输差错问题，其中，节点只做帧的转发操作，不需要执行接收确认和请求重发等操作，差错控制和流量控制均交由上层协议完成，所以大大缩短了节点的时延，提高了网内数据的传输速率。这主要是因为目前帧中继技术所使用的广域网环境比起 20 世纪七八十年代 X.25 协议普及时所存在的网络基础设施，无论在服务的稳定性还是质量方面都有了很大的提高和改进。帧中继是一种严格意义上的第二层协议，所以可以把一些复杂的控制和管理功能交由上层协议完成。这样就大大提高了帧中继的性能和传输速度，使其更加适合广域网环境下的各种应用。

考虑到一个连锁公司，在全国有 3 个分支机构。分支机构的广域网连接使用专线（使用专线主要是出于安全和性能方面的考虑），为了提供最大限度的相互容错能力，分支机构间采用全互连的拓扑，需要申请 3 条专线来互连各个分支机构，每个分支机构的接入路由器需要配备两个广域网接口来连接专线，如图 16-1-1 所示。公司如果有 10 个分支机构，仍然采用全互连的技术，将需要 $10 * (10 - 1) / 2 = 45$ 条专线，每个分支机构的接入路由器将需要配置 9 个广域网接口。这样通过专线全互连的方式，不管是专线链路的租用费用，还是配置如此高档路由器的费用，都相当惊人，且随着公司规模的扩大，专线数和所有路由器的接口数都要随之增加，极易造成设备的淘汰和运营成本的增加。

专线全互连的方式制约着公司规模的扩大。此时可以考虑使用一种新的广域网技术——帧中继，在帧中继网络中使用 VC（Virtual Circuit，虚电路）来互连各个分支机构。这种使用虚电路互连各个分支机构的方式，并不需要每两个分支机构间有单独的物理链路，各个分支机构通过物理链路连接到帧中继网络，帧中继网络一般都是由网络运营商提供和维护的，用户只需要向网络运营商申请虚电路来互连各个分支机构即可，如图 16-1-2 所示。

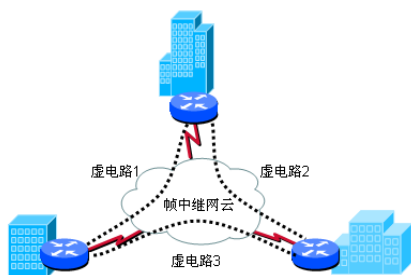


图 16-1-2 帧中继全互连方式

16.1.2 帧中继术语***

本章涉及的所有帧中继配置在 Dynamips 的 CCNA 机架完成。打开光盘中的“配置\16\R2-帧中继.txt”文件，把文本内容粘贴到路由器 R2 上，如图 16-1-4 所示，把路由器 R2 配置成帧中继交换机。CCNA 考试中不涉及如何把路由器配置成帧中继交换机，读者可以不用理会图 16-1-4 中的配置，但理解图 16-1-4 中的配置有助于读者明白帧中继的工作方式，本章稍后对图 16-1-4 中的配置进行解释。路由器 R1、R3 和 R4 使用串行线缆连接到帧中继交换机。

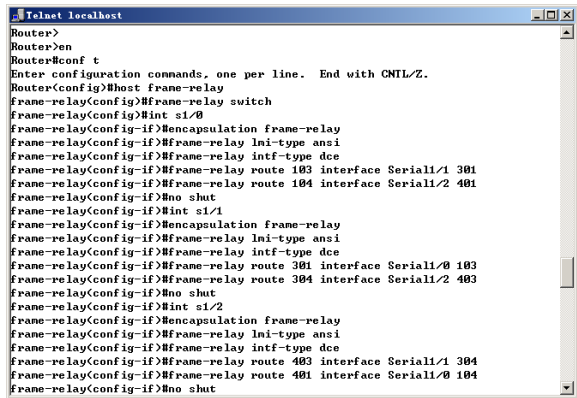


图 16-1-4 把路由器 R2 配置成帧中继交换机

1. VC (Virtual Circuit, 虚电路)

433

动态地建立虚电路，这样建立的链路称为交换虚电路（Switched Virtual Circuit, SVC），有点像动态路由协议，可以自行调整路径。但 SVC 并不常用，CCNA 考试中也不涉及这一内容。更常使用的是永久虚电路（Permanent Virtual Circuit, PVC），PVC 由运营商预先静态配置，有点像静态路由协议需管理员手工维护。在图 16-1-3 中，R1 和 R3 之间、R1 和 R4 之间、R3 和 R4 之间，各存在一条 PVC。

2. 数据链路连接标识符（Data Link Connection Identifier, DLCI）

DLCI 是源设备和目的设备之间标识逻辑电路的一个数据值，该数值只具有本地意义，比如在图 16-1-3 中，R1 上的 DLCI 号 103 标识的是 R1 到 R3 的连接，R1 上的 DLCI 号 104 标识的是 R1 到 R4 的连接。不同 DTE 设备上的 DLCI 号可以相同，比如 R3 完全可以用 DLCI 号 103 来标识到 R4 的连接。但在同一台 DTE 设备上，不能使用同一个 DLCI 号来标识到不同目的设备的连接。

帧中继交换机通过在点对路由器之间映射 DLCI 来创建永久虚电路。比如在图 16-1-3 中，帧中继交换机 R2 可以在 R1 的 103 和 R3 的 301 之间进行映射来提供一条永久的虚电路，R1 只要封装 DLCI 号 103，发出的数据帧就可以到达 R3，R3 只要封装 DLCI 号 301，发出的数据帧就可以到达 R1。本书的实验中，只有一台路由器 R2 来模拟一台帧中继交换机，在实际的环境中，中间是一个帧中继网云，帧中继网云中包括多台帧中继交换机，帧中继交换机之间有预先配置的约定，可以把源设备的数据帧最终交换到目的设备。类似的帧中继交换机 R2 在 R1 的 104 和 R4 的 401 之间进行映射来提供一条永久的虚电路，在 R3 的 304 和 R4 的 403 之间进行映射来提供一条永久的虚电路。

DLCI 地址空间限制为 10bits，产生了 1024 个可用 DLCI。可用的 DLCI 号与下面将要介绍的 LMI 类型有关。Cisco LMI 类型支持 16~1007 范围内的 DLCI 携带用户数据，ANSI/Q933A LMI 类型支持 16~992 范围内的 DLCI 携带用户数据。DLCI 号 0~15 和 1008~1023 被保留用于特殊的用途，部分用于 LMI 消息和组播地址，比如 LMI 类型是 ANSI 和 Q933A 的 LMI 消息使用的 DLCI 号是 0，而 LMI 类型是 Cisco 的 LMI 消息使用的 DLCI 号是 1023。

3. 本地管理接口（Local Management Interface, LMI）

LMI 是用户端设备和帧中继交换机之间的信令标准，负责管理设备之间的连接，维护设备之间的状态。

（1）LMI 的主要作用

- 获知路由器被分配了哪些 DLCI，确定 PVC 的操作状态，有哪些可用的 PVC 等。

DTE 端的思科路由器定期（每 10 秒）向帧中继交换机发送 **LMI 状态查询** 消息，帧中继交换机进行响应，这种消息有保持激活功能，允许两台设备确定彼此的状态。思科路由器每隔 5 个状态查询后（也就是每 60 秒）会发送一个 **LMI 完全状态查询**，向帧中继交换机询问完全的状态信息，包括所有 PVC 信息、DLCI 号、配置的速率和状态等。在图 16-1-3 中，R1 借助 LMI，可以获知被分配了两个 DLCI，即 103 和 104。运行 Dynamips 机架上的 R1、R2、R3 和 R4，它们之间的连接如图 16-1-5 所示。

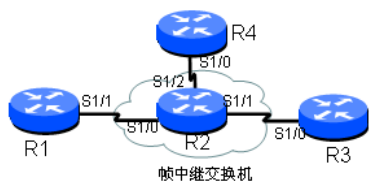


图 16-1-5 帧中继连接接口

R2 的配置如图 16-1-4 所示，R1 的配置如下：

```
Router>en
Router#conf t
Router(config)# host R1
R1(config)#int s1/1
R1(config-if)# encapsulation frame-relay
```

封装帧中继。帧中继有两种封装类型，cisco 和 ietf，默认的封装类型是 cisco，如果连接到一台非思科的设备，帧中继的封装类型要使用 ietf，也就是使用“encapsulation frame-relay ietf”命令。

```
R1(config-if)#no shut
```

配置完 R1 后，在 R1 上使用“show frame-relay pvc”命令，查看 DLCI 的分配情况，显示如下：

```
R1#show frame-relay pvc
PVC Statistics for interface Serial1/1 (Frame Relay DTE)
      Active      Inactive      Deleted      Static
Local          0            0            0            0
Switched       0            0            0            0
Unused         0            2            0            0
DLCI = 103, DLCI USAGE = UNUSED, PVC STATUS = INACTIVE, INTERFACE = Serial1/1

input pkts 0          output pkts 0          in bytes 0
out bytes 0          dropped pkts 0          in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0        in BECN pkts 0        out FECN pkts 0
out BECN pkts 0        in DE pkts 0          out DE pkts 0
out bcast pkts 0      out bcast bytes 0
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 01:14:52, last time pvc status changed 01:14:52

DLCI = 104, DLCI USAGE = UNUSED, PVC STATUS = INACTIVE, INTERFACE = Serial1/1

input pkts 0          output pkts 0          in bytes 0
out bytes 0          dropped pkts 0          in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0        in BECN pkts 0        out FECN pkts 0
out BECN pkts 0        in DE pkts 0          out DE pkts 0
out bcast pkts 0      out bcast bytes 0
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 01:15:16, last time pvc status changed 01:15:16
```

从上面的输出中可以看出，R1 已经使用 LMI 从帧中继交换机学到了本地可用的 DLCI 号 103 和 104。DLCI 使用情况都是“UNUSED”，即没有使用。PVC 状态都是“INACTIVE”，即不可用，这是因为 PVC 在两端 DLCI 都可用的情况下，才能映射出一条虚电路。PVC 的状态有 3 种：ACTIVE 表示正常；INACTIVE 一般是远端配置有问题，如远端路由器没有开启、帧中继交换机远端的接口配置错误等；DELETED 一般是近端配置有问题，如路由器配置了一个并不存在的 DLCI 号等。

继续运行 R3，配置如下：

```
Router>en
Router#conf t
Router(config)# host R3
R3(config)#int s1/0
R3(config-if)#encapsulation frame-relay
```

在思科路由器上接口帧中继的封装类型默认是 cisco，如果远端的设备是非思科路由器，这里要使用“encapsulation frame-relay ietf”命令，否则两端的封装类型不一致，网络协议将失败。

```
R3(config-if)#no shut
```

再次查看 R1 上的帧中继 PVC，关键部分显示如下：

```
R1#show frame-relay pvc
DLCI = 103, DLCI USAGE = UNUSED, PVC STATUS = ACTIVE, INTERFACE = Serial1/1
DLCI = 104, DLCI USAGE = UNUSED, PVC STATUS = INACTIVE, INTERFACE = Serial1/1
```


从上面的输出中，注意到 R1 和 R3 之间的 PVC 状态已经是 ACTIVE，即 PVC 建立成功。而 R3 和 R4 之间 PVC 尚未建立，主要是因为 R4 尚未配置。配置 R4 如下：

```
Router>en
Router#conf t
Router(config)# host R4
R4(config)#int s1/0
R4(config-if)#encapsulation frame-relay
R4(config-if)#no shut
```

稍后查看 R1、R3、R4，发现所有的 PVC 状态都是 ACTIVE，即所有的 PVC 都建立成功。因为还没有配置 IP 地址，所有 PVC 都没有使用“UNUSED”。

- 发送维持分组，以确保 PVC 处于激活状态。

读者可以关闭路由器 R3 的 S1/0 接口，大约一分钟左右，再次查看 R1 上 PVC 状态，可以发现“DLCI = 103, DLCI USAGE = UNUSED, PVC STATUS = INACTIVE, INTERFACE = Serial1/1”，DLCI 号 103 对应的 PVC 状态变成了不可用。

(2) LMI 类型

LMI 有 3 种类型：ANSI、Cisco、Q933A。DTE 端（一般是用户端路由器）LMI 的类型只要与帧中继交换机上相连接口的 LMI 类型配置一致即可，与远端帧中继交换机接口的 LMI 类型和远端路由器接口的 LMI 类型无关，所以 LMI 被称为 Local，和 DLCI 一样，也是只有本地意义。如果 LMI 类型不一致将导致 PVC 失败。使用下面的命令更改 LMI 的类型：

```
R3(config-if)#frame-relay lmi-type ?
cisco
ansi
q933a
```

在思科路由器上，默认的 LMI 类型是 Cisco。思科路由器上可以不用配置 LMI 类型，从 IOS11.2 开始，Cisco 路由器能自动感知帧中继交换机上配置的 LMI 类型。路由器为每个 LMI 类型向帧中继交换机发送状态查询，并等待查看帧中继交换机回应哪个查询。路由器会根据帧中继交换机上 LMI 的类型，自动调整路由器的 LMI 类型。从图 16-1-4 中，可以看到帧中继交换机上使用的 LMI 类型是 ANSI，使用“show frame-relay lmi”命令查看路由器 R1 接口的 LMI 类型，显示如下：

```
R1#show frame-relay lmi

LMI Statistics for interface Serial1/1 (Frame Relay DTE) LMI TYPE = ANSI
Invalid Unnumbered info 0          Invalid Prot Disc 0
Invalid dummy Call Ref 0          Invalid Msg Type 0
Invalid Status Message 0          Invalid Lock Shift 0
Invalid Information ID 0          Invalid Report IE Len 0
Invalid Report Request 0          Invalid Keep IE Len 0
Num Status Enq. Sent 3            Num Status msgs Rcvd 3
Num Update Status Rcvd 0          Num Status Timeouts 0
Last Full Status Req 00:00:38     Last Full Status Rcvd 00:00:38
```

从上面的输出中可以看出，R1 的 S1/1 接口的 LMI 类型不再是默认的 Cisco，而是根据帧中继交换机上的配置自动调整成了 ANSI。如果读者手工把两端配置成不一致的 LMI 类型，取消它们的自动调整，不一致的 LMI 类型将导致 LMI 失败，进而导致 PVC 失败。“Num Status Enq. Sent”表示路由器发出的 LMI 状态查询的次数，“Num Status msgs Rcvd”表示路由器收到帧中继交换机对 LMI 状态查询应答的次数，“Num Update Status Rcvd”表示收到帧中继交换机 LMI 完全状态查询应答的次数，“Num Status Timeouts”表示路由器发送查询却没有收到应答的次数，“Last Full Status Req”是距离最后一次发送 LMI 完全状态查询

时间，这个值正常不会超过 60 秒。如果 Invalid（非法）字段的值不断增加，多数是两端配置了不一致的 LMI 类型。

（3）LMI 扩展

除了为传输数据定义基本帧中继协议功能之外，帧中继规范还包括 LMI 扩展，它使得对大规模的复杂互连网络的支持变得更容易。LMI 扩展包括：虚电路状态消息、组播、全局寻址、简单流量控制，CCNA 考试中不涉及这一内容。

4. 承诺信息速率（Committed Information Rate, CIR）

承诺信息速率是服务提供商承诺要提供的有保证的速率，以 b/s 为单位。

5. 承诺突发（Committed Burst, BC）

在承诺信息速率的测量间隔内，交换机准许接收和发送的最大数据量，以 b/s 为单位。

6. 超量突发（Excess Burst, BE）

在承诺信息速率之外，帧中继交换机试图发送的未承诺的最大额外数据量，也是以 b/s 为单位。超量突发依赖于运营商提供的服务，把超量突发数据看做可丢弃的数据。

7. 前向显示拥塞通知（Forward Explicit Congestion Notification, FECN）

帧中继设置的一个比特，用以通知 DTE 接收设备应启动拥塞避免程序。当帧中继交换机识别出网络中发生拥塞时，把帧中 FECN 比特位设置为“1”，暗示拥塞发生。

8. 后向显示拥塞通知（Backward Explicit Congestion Notification, BECN）

帧中继设置的一个比特，用以通知 DTE 发送设备应启动拥塞避免程序。当帧中继交换机识别出网络中发生拥塞时，它就向原路由器发送一个 BECN 分组，指示该路由器降低发送分组的速率，如果路由器在当前时间间隔内收到 BECN，则将传输速率降低 25%。

9. 允许丢弃（Discard Eligibility, DE）

一个设定比特，指示在拥塞发生时本帧可被丢弃。当路由器检测到网络拥塞时，帧中继交换机将首先丢弃设置了 DE 比特的分组。超出 CIR 的那部分流量将被设置 DE 比特。

16.1.3 帧中继运行方式*

这里介绍一下帧中继是如何工作的。在如图 16-1-6 所示的帧中继网络中，R1、R3、R4 通过帧中继实现全互连。R1 是怎样实现把数据包直接发往 R3 的呢？

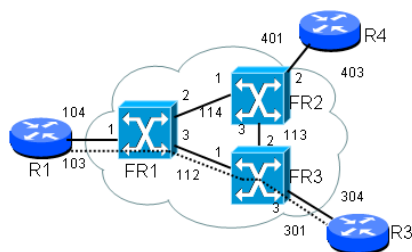


图 16-1-6 帧中继工作方式

1. 帧中继帧格式

这里先回顾一下以太网的帧，以太网帧格式如图 16-1-7 所示。

字节数	1	2	6	2	46~1500	4
字段域	Preamble (前导位)	Destination Address (目的 MAC地址)	Source Address (源 MAC地址)	Length / Type (长 度/类型)	802.2 Header and Data (802.2 头部和数据)	Frame Check Sequence (帧 检验序列)

图 16-1-7 以太网帧格式

帧中继的帧和以太网的帧一样，也工作在数据链路层，帧中继帧的格式如图 16-1-8 所示。

字节数	1	2	可变的	2	1
字段域	Flag (帧开始标志)	地址, 包括 DLCI、FECN、BECN 和 DE 位	Data (数据)	Frame Check Sequence (帧检验序列)	Flag (帧结束标志)

图 16-1-8 帧中继帧格式

帧中继的字段域如下：

- (1) 标志 (Flag)：标志帧中继数据帧的开始和结束。
- (2) 地址 (Address)：帧中继的地址字段有 2 个字节，即 16 个比特。包含下列信息：
 - DLCI 值。指示 DLCI 的值，帧中继和以太网不同，有目的 MAC 地址和源 MAC 地址之分，帧中继的帧中只有一个 DLCI 号，代表要去往的目的地。地址字段中有 10 个比特用来表示 DLCI 号。
 - 拥塞控制 (Congestion Control)。地址字段中有 3 个比特，用来实现帧中继的拥塞通知机制，包括 1 个比特的 FECN 位、1 个比特的 BECN 位，以及 1 个比特的 DE 位。
 - 其他值。地址域中还包括 3 个比特的其他字段域。
- (3) 数据 (Data)：是一个可变长度的字段，包含封装的上层协议数据。
- (4) 帧校验序列 (FCS)：用来保证传输数据的完整性。

2. 帧中继中的帧转发

在图 16-1-6 中，假设 R1 要把数据包发往 R3，R1 封装 DLCI 号 103（至于 R1 如何知道去往 R3 要封装 DLCI 号 103，接下来将介绍），把帧发往帧中继交换机 FR1。

帧中继的帧到达帧中继交换机 FR1，FR1 根据管理员的配置，知道如果从端口 1 收到 DLCI 号 103 的帧，应该把 DLCI 号修改成 112，并从 3 号端口发出。

帧中继的帧到达帧中继交换机 FR3，FR3 根据管理员的配置，知道如果从端口 1 收到 DLCI 号 112 的帧，应该把 DLCI 号修改成 301，并从 3 号端口发出。

R3 接收到 FR3 发过来的帧中继帧，解封装后交给上层协议处理。从上面的工作方式中可以看出，只要 R1 用 DLCI 号 103 封装帧中继的帧，就可以把数据发送到 R3。同理，R3 只要用 DLCI 号 301 封装帧中继的帧，就可以把数据发送到 R1。帧中继网云使用 DLCI 号 103、112 和 301 在 R1 和 R3 之间建立了一条永久的虚电路。

3. 帧中继交换表

从上面帧中继帧的转发过程，可以看到在 FR1 和 FR3 帧中继交换机上并没有检测到数据包的 IP 层，仅仅执行了 DLCI 的重新映射。在 FR1 和 FR3 上都维护着帧中继的交换表，其中 FR1 的帧中继交换表如表 16-1-1 所示。

表 16-1-1 FR1 的帧中继交换表

入站端口	入站 DLCI	出站端口	出站 DLCI
1	103	3	112
1	104	2	114
2	114	1	104
3	112	1	103

4. 路由器配置成帧中继交换机

下面来讲解一下把路由器 R2 配置成帧中继交换机的命令，只不过这个帧中继网络中只有一台帧中继交换机。配置和解释如下：

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host frame-relay
frame-relay(config)#frame-relay switch           把路由器配置成帧中继交换机。
frame-relay(config)#int s1/0
frame-relay(config-if)#encapsulation frame-relay 使用帧中继封装。
frame-relay(config-if)#frame-relay lmi-type ansi
帧中继 LMI 的类型是 ANSI，如果不指定类型，默认是 cisco。这句是可选配置。
frame-relay(config-if)#frame-relay intf-type dce
帧中继的接口类型是 DCE，这和具体连接是 DTE 还是 DCE 线缆无关。为了帧中继交换，需要把它改变成 DCE，
路由器默认是 DTE。
frame-relay(config-if)#frame-relay route 103 interface Serial1/1 301
R2 把从 S1/0 接口接收的 DLCI 号为 103 的帧中继帧经由 S1/1 接口的路线上转发出去，并把 DLCI 号更换成 301。
frame-relay(config-if)#frame-relay route 104 interface Serial1/2 401
R2 把从 S1/0 接口接收的 DLCI 号为 104 的帧中继帧经由 S1/2 接口的路线上转发出去，并把 DLCI 号更换成 401。
frame-relay(config-if)#no shut
frame-relay(config-if)#int s1/1
frame-relay(config-if)#encapsulation frame-relay
frame-relay(config-if)#frame-relay lmi-type ansi
frame-relay(config-if)#frame-relay intf-type dce
frame-relay(config-if)#frame-relay route 301 interface Serial1/0 103
R2 把从 S1/1 接口接收的 DLCI 号为 301 的帧中继帧经由 S1/0 接口的路线上转发出去，并把 DLCI 号更换成
103。这里的配置刚好和前面 S1/0 接口下的配置对称起来。
frame-relay(config-if)#frame-relay route 304 interface Serial1/2 403
frame-relay(config-if)#no shut
frame-relay(config-if)#int s1/2
frame-relay(config-if)#encapsulation frame-relay
frame-relay(config-if)#frame-relay lmi-type ansi
frame-relay(config-if)#frame-relay intf-type dce
frame-relay(config-if)#frame-relay route 403 interface Serial1/1 304
frame-relay(config-if)#frame-relay route 401 interface Serial1/0 104
frame-relay(config-if)#no shut
```

16.1.4 帧中继寻址***

16.1.3 节中提到 R1 要把数据包发往 R3，将封装 DLCI 号 103，R1 是如何知道要封装 103 的呢？继续配置 R1、R2 和 R3 接口的 IP 地址。R1 的配置如下：

```
R1(config)#int s1/1
R1(config-if)#ip add 123.1.1.1 255.255.255.0
R3 的配置如下：
R3(config)#int s1/0
R3(config-if)#ip add 123.1.1.3 255.255.255.0
R4 的配置如下：
R4(config)#int s1/0
R4(config-if)#ip add 123.1.1.4 255.255.255.0
```

配置完成，大约一分钟左右，使用“show frame-relay map”命令查看 R1 上的帧中继映射，显示如下：

```
R1#show frame-relay map
Serial1/1 (up): ip 123.1.1.3 dlci 103(0x67,0x1870), dynamic,
                broadcast,
                CISCO, status defined, active
Serial1/1 (up): ip 123.1.1.4 dlci 104(0x68,0x1880), dynamic,
                broadcast,
                CISCO, status defined, active
```

从上面的输出中, 可以看到去往 R3 (123.1.1.3 的数据包), 封装的 DLCI 号应该是 103, “dynamic” 表示这种映射关系是动态学来的; “broadcast” 表示帧中继链路上支持广播; 帧中继的封装类型是 “cisco”; “active” 表示链路正常。

同样, R1 还学到了去往 R4 (123.1.1.4) 的 DLCI 号是 104。

1. 反向 ARP (Inverse ARP)

在帧中继链路上, 从 DLCI 号解析出 IP 地址是由反向 ARP 完成的 (考试中一定要选择 Invers ARP, 不要错误的选择 RARP, RARP 用在以太网上)。反向 ARP 机制允许路由器自动建立帧中继映射, 该映射将 DLCI 和路由器的网络地址相关联。反向 ARP 在非手工配置的激活 VC 上每 60 秒发生一次, 这就是前面配置完成后, 为什么要等大约一分钟左右的原因。

2. 反向 ARP 解析过程

这里以图 16-1-3 中 R1 解析 R3 (123.1.1.3) 的过程为例, 讲解反向 ARP 的解析过程, 该解析过程如图 16-1-9 所示。

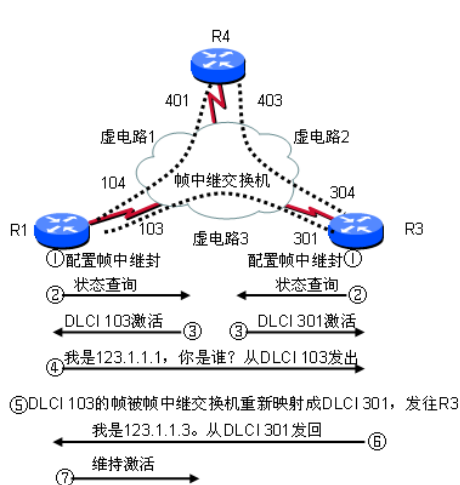


图 16-1-9 反向 ARP 解析过程

① 配置帧中继封装。

② 路由器向帧中继交换机发送状态查询信息。该消息既可以向交换机通知路由器的状态, 又可以向交换机询问有哪些可用的 DLCI 号。

③ 帧中继交换机通知路由器 R1, DLCI 号 103 和 104 是激活的, 可以使用。

④ 对于每一个激活状态的 DLCI, 路由器 R1 都发送一个反向 ARP 请求分组。用来介绍自己的当前状态, 同时也请求远程路由器发送网络层地址来进行响应。这里 R1 要发送两个这样的请求包, 封装的 DLCI 号分别是 103 和 104, 从这里可以看出帧中继网络是不支持广播的, 因为从帧中继链路上发出的数据包必须有 DLCI 号, DLCI 号限制了该帧只能到达一个目的地址。帧中继的网络默认是 NBMA (Non-Broadcast Multiple Access, 非广播多路访问), 通过发送帧的多个拷贝来解决广播问题。这里仅以 DLCI 号 103 为例。

⑤ 帧中继网云 (这里只有一台帧中继交换机 R2) 把 DLCI 号 103 重新映射成 301, 并把该帧从 S1/1 接口发出。

⑥ R3 收到帧中继交换机发过来的帧, 帧的 DLCI 号是 301。R3 处理该数据帧, 并进行应答, 封装的帧是进入的帧 301, 告知对方自己的 IP 地址是 123.1.1.3。

⑦ R3 应答的帧被帧中继交换机 (路由器 R2) 重新映射成 103 从 S1/0 接口发出, R1 接收到该帧, 帧的 DLCI 号是 103, 网络层通告的 IP 地址是 123.1.1.3。R1 在本地的映射表中添加 123.1.1.3 和对应的 DLCI 号 103, 以后有发往 123.1.1.3 的数据帧, 就用 DLCI 号 103 进行封装。R1 继续发送维持消息 (此间隔默认是 10 秒, 反向 ARP 默认发送的间隔是 60 秒), 验证帧中继交换机是否仍处于激活状态。

同理, R1、R3、R4 都可以学到对方的 IP 地址和对应的 DLCI 号。

16.1.5 水平分割问题***

1. 帧中继的拓扑类型

有时出于费用和应用方面的考虑，可能不需要建立全互连的帧中继网络，只需建立部分互连或星型互连（Hub and Spoke，所有路由器都连接到中心场点）网络即可。如图 16-1-10 所示，A 是全网状互连；B 是星型互连；C 是部分网状互连。

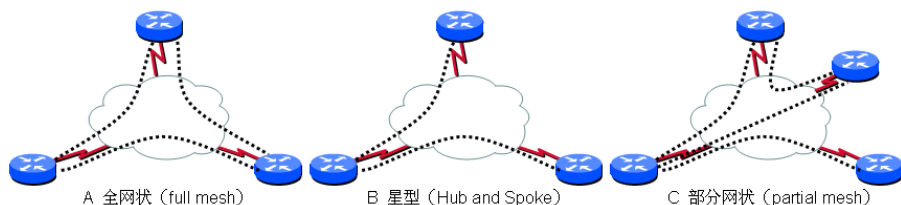


图 16-1-10 帧中继的网络类型

2. 路由可达性问题

以图 16-1-10 中的星型拓扑为例，配置 RIP 路由协议。Spoke 端把路由信息发送给 Hub 路由器，因为水平分割的原因，Hub 路由器不会把从一个接口学到的路由再从这个接口发出去，结果造成 Hub 路由器可以学到所有分支机构的路由，但分支机构之间相互学不到对方的路由。

解决这种路由可达性问题的方法有四种：

- 一是全网互连（因涉及费用，算不上是一种方法）。
- 二是使用静态路由（缺少了动态路由的优点，也算不上是一种方法）。
- 三是关闭水平分割。
- 四是使用子接口。

3. 子接口类型

可以将子接口配置成下列连接类型：

- **点到点 (Point-to-Point)：** 使用一个单独的子接口来建立一条 PVC，该 PVC 连接到一台远程路由器的子接口或物理接口。在这种情况下，路由器的多个子接口分别属于不同的网络，每个子接口都有单独的 DLCI。
- **多点子接口 (Multipoint)：** 使用一个单独的子接口来建立多条 PVC，这些 PVC 连接到远程路由器的子接口或物理接口。在这种情况下，所有连接到这个子接口的远程路由器的子接口或物理接口的 IP 地址同属于一个子网。这里的多点子接口和物理接口一样，仍然会受到水平分割的限制。

点到点子接口可以解决路由的水平分割问题，但因为要使用多个子网，会造成 IP 地址的浪费。多点子接口和物理接口一样，连接的多个远程设备同属于一个子网，虽然节省了 IP 地址的使用，但存在路由的水平分割问题。本章下一节介绍点到点和多点子接口的配置。

16.2 配置帧中继***

本节介绍帧中继的基本配置和查看命令、水平分割造成路由可达性问题和使用子接口的解决办法。

16.2.1 帧中继基本配置**

配置图 16-2-1 中的帧中继网络，R1 S1/1 的 IP 地址是 134.1.1.1，R3 S1/0 的 IP 地址是 134.1.1.3，R4 S1/0 的 IP 地址是 134.1.1.4。配置帧中继，实现全网全通（任何 IP 地址之间均可 ping 通，包括 ping 路由器本端的 IP 地址）。

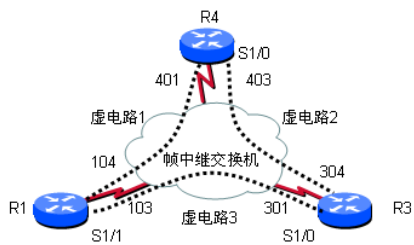


图 16-2-1 配置帧中继

1. 配置

运行 Dynamips CCNA 机架上的 R1、R2、R3 和 R4。帧中继交换机（路由器 R2）的配置如图 16-1-4 所示。

R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#encapsulation frame-relay
R1(config-if)#ip add 134.1.1.1 255.255.255.0
R1(config-if)#no shut
```

R3 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#enca fram
R3(config-if)#ip add 134.1.1.3 255.255.255.0
R3(config-if)#no shut
```

R4 的配置如下：

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with C
Router(config)#host R4
R4(config)#int s1/0
R4(config-if)#enca fram
R4(config-if)#ip add 134.1.1.4 255.255.255.0
R4(config-if)#no shut
```

2. 测试

读者在 R1 上 ping 134.1.1.3 和 134.1.1.4，验证网络的连通性。如果 ping 不通，稍候大约一分钟后再试，因为反向 ARP 默认发送的间隔是 60 秒。如果仍然 ping 不通，使用“show frame-relay map”命令，查看 IP 地址到 DLCI 号的映射情况，如果都正确，应该可以有下面的输出。

```
R1#show frame-relay map
Serial1/1 (up): ip 134.1.1.3 dlci 103(0x67,0x1870), dynamic,
broadcast,, status defined, active
Serial1/1 (up): ip 134.1.1.4 dlci 104(0x68,0x1880), dynamic,
broadcast,, status defined, active
```

如果 IP 地址到 DLCI 号的映射与上面列出的不同，请进一步查看 PVC 的运行情况。使用的命令是“show frame-relay pvc”，正确的显示如下：

```
R1#show frame-relay pvc
```


PVC Statistics for interface Serial1/1 (Frame Relay DTE)

	Active	Inactive	Deleted	Static
Local	2	0	0	0
Switched	0	0	0	0
Unused	0	0	0	0

DLCI = 103, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial1/1

```
input pkts 6          output pkts 6          in bytes 554
out bytes 554         dropped pkts 0        in pkts dropped 0
out pkts dropped 0    out bytes dropped 0
in FECN pkts 0        in BECN pkts 0        out FECN pkts 0
out BECN pkts 0        in DE pkts 0          out DE pkts 0
out bcast pkts 1      out bcast bytes 34
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 00:07:40, last time pvc status changed 00:06:10
```

DLCI = 104, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial1/1

```
input pkts 4          output pkts 4          in bytes 346
out bytes 346         dropped pkts 0        in pkts dropped 0
out pkts dropped 0    out bytes dropped 0
in FECN pkts 0        in BECN pkts 0        out FECN pkts 0
out BECN pkts 0        in DE pkts 0          out DE pkts 0
out bcast pkts 1      out bcast bytes 34
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 00:07:41, last time pvc status changed 00:05:41
```

如果 R1 学不到 DLCI 号，请检测路由器 R1 的物理端口有没有打开，封装的协议是不是帧中继，LMI 的类型是否与交换机端的配置不一致。在路由器 R1 上使用“show int s1/1”命令进行验证，显示如下：

```
R1#show int s1/1
Serial1/1 is up, line protocol is up
Hardware is M4T
Internet address is 134.1.1.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY, crc 16, loopback not set
Keepalive set (10 sec)
Restart-Delay is 0 secs
LMI enq sent 88, LMI stat recvd 89, LMI upd recvd 0, DTE LMI up
LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
LMI DLCI 0 LMI type is ANSI Annex D frame relay DTE
```

如果看到 PVC 的状态不是“ACTIVE”，则表示 PVC 状态有问题。“INACTIVE”表示可能是远端有问题，比如帧中继没有打开远端的接口，远端的 DTE 路由器配置有问题等。“DELETED”表示可能是近端的配置有问题，比如用户配置一个不存在的 DLCI 号或交换机删除了相关的 DLCI 号等。

3. 帧中继 ping 通本端

在路由器 R1 上 ping 134.1.1.1，结果如何呢？读者可能会认为一定是通的，因为远端都能 ping 通，ping 通本端应该没有问题。测试显示如下：

```
R1#ping 134.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 134.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

居然 ping 不通，有点出人意料吧。ping 134.1.1.1 时，帧中继试图找到 DLCI 号和 IP 地址映射，没有找到，结果失败。解决的办法是把 DLCI 号和 IP 地址之间做一个静态映射，配置如下：

```
R1(config-if)#frame-relay map ip 134.1.1.1 103 broadcast
```

该命令的完整格式如下：

```
Router(config-if)#frame-relay map ip ip 地址 DLCI 号 [broadcast] [cisco|ietf]
```

该命令的作用是把 IP 地址与 DLCI 号之间做一个静态映射。IP 地址是要去的目的地址，DLCI 号是本地链路标识号。broadcast 是一个可选的关键字，让链路支持广播，配置动态路由协议时，该关键字不可以省略，否则动态路由选择协议生成的路由选择更新不会通过 PVC。最常见的配置是，不管要不要运行动态路由协议，broadcast 选项都配上。如果使用的不是思科设备，ietf 选项要配置。

查看 R1 DLCI 号和 IP 地址的映射表，显示如下：

```
Serial1/1 (up): ip 134.1.1.1 dlci 103(0x67,0x1870), static,
                broadcast,
                CISCO, status defined, active
Serial1/1 (up): ip 134.1.1.3 dlci 103(0x67,0x1870), dynamic,
                broadcast,, status defined, active
Serial1/1 (up): ip 134.1.1.4 dlci 104(0x68,0x1880), dynamic,
                broadcast,, status defined, active
```

注意，在路由器 R1 上有一个静态（static）映射。再次在 R1 上 ping 134.1.1.1，显示如下：

```
R1#ping 134.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 134.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/52/72 ms
```

此时 R1 可以 ping 通本端了。“frame-relay map ip 134.1.1.1 103 broadcast”命令在 R1 上把 134.1.1.1 和 DLCI 103 进行映射，R1 把去往 134.1.1.1 的包封装 DLCI 103 发送出去，该帧中继帧到达路由器 R3 后，R3 得知目的 IP 地址是 134.1.1.1，R3 查询本地的映射表，知道去往 134.1.1.1 的包要封装 DLCI 号 301，R3 把重新封装后的帧发往帧中继交换机，最后 R1 收到应答帧，ping 测试成功。从这里可以看出，R1 虽然 ping 的是本端 IP 地址，数据包却是到达了远端又返回来的，如果关闭 R3 的 S1/0 接口，R1 ping 本端将失败。同样也可以把 134.1.1.1 映射成 104，即发往 R4。

同理，如果 R3 和 R4 也需要 ping 通本端，同样需要做类似的静态映射。

4. 静态映射配置

有时，在某些情况不允许使用反向 ARP。使用下面的命令关闭 R1、R3 和 R4 的反向 ARP：

```
R1(config)#int s1/1
R1(config-if)#no frame-relay inverse-arp

R3(config)#int s1/0
R3(config-if)#no frame-relay inverse-arp

R4(config)#int s1/0
R4(config-if)#no frame-relay inverse-arp
```

此时 R1、R3、R4 之间仍然可以 ping 通，这是因为之前使用反向 ARP 建立的映射依然存在，使用下面的命令清除使用反向 ARP 学到的动态映射：

```
R1#clear frame-relay inarp
R1#show frame-relay map
Serial1/1 (up): ip 134.1.1.1 dlci 103(0x67,0x1870), static,
                broadcast,
                CISCO, status defined, active
```

清除反向 ARP 后，可以发现只有静态映射的条目仍然存在。此时 R1 无法 ping 通 R3 和 R4，解决的办法是全部使用静态映射来代替动态映射。

R1 的配置如下：

```
R1(config)#int s1/1
R1(config-if)#frame-relay map ip 134.1.1.3 103 broadcast
R1(config-if)#frame-relay map ip 134.1.1.4 104 broadcast
```

R3 的配置如下：

```
R3(config)#int s1/0
R3(config-if)#frame-relay map ip 134.1.1.1 301 broadcast
R3(config-if)#frame-relay map ip 134.1.1.3 301 broadcast
R3(config-if)#frame-relay map ip 134.1.1.4 304 broadcast
```

R4 的配置如下：

```
R4(config)#int s1/0
R4(config-if)#frame-relay map ip 134.1.1.1 401 broadcast
R4(config-if)#frame-relay map ip 134.1.1.4 401 broadcast
R4(config-if)#frame-relay map ip 134.1.1.3 403 broadcast
```

此时，R1、R3 和 R4 没有使用反向 ARP，仍然可以 ping 通本端和远端。查看 R1 的帧中继映射表，显示如下：

```
R1#show frame-relay map
Serial1/1 (up): ip 134.1.1.1 dlci 103(0x67,0x1870), static,
                broadcast,
                CISCO, status defined, active
Serial1/1 (up): ip 134.1.1.3 dlci 103(0x67,0x1870), static,
                broadcast,
                CISCO, status defined, active
Serial1/1 (up): ip 134.1.1.4 dlci 104(0x68,0x1880), static,
                broadcast,
                CISCO, status defined, active
```

R3 和 R4 的显示与 R1 的显示类似。

16.2.2 RIP over 帧中继**

帧中继作为二层链路，上面可以运行各种动态路由协议，这里仅以 RIP 为例。帧中继上运行 OSPF 的情况要复杂得多，属于 CCNP 的内容。

配置图 16-2-2 中的路由器，R1 S1/1 的 IP 地址是 134.1.1.1，R3 S1/0 的 IP 地址是 134.1.1.3，R4 S1/0 的 IP 地址是 134.1.1.4。配置帧中继，实现全网全通。要求：仅允许使用图中出现的 PVC。

在图 16-2-2 中，帧中继交换机上已经配置了 3 条虚电路，如果使用反向 ARP，R3 和 R4 之间的 PVC 也将被使用，这与要求不符。在实际的环境中，经常出于费用或需求方面的考虑，也不使用全互连的连接。图 16-2-2 中采用的是星型连接，这种连接拓扑典型用在总部和多个分支机构场景中。

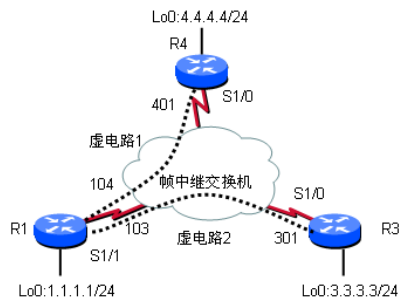


图 16-2-2 RIP over 帧中继

首先配置帧中继，帧中继交换机（路由器 R2 的配置同前），R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#enca frame-relay
R1(config-if)#no frame-relay inverse-arp
R1(config-if)#ip add 134.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#frame-relay map ip 134.1.1.1 103 broadcast
R1(config-if)#frame-relay map ip 134.1.1.3 103 broadcast
R1(config-if)#frame-relay map ip 134.1.1.4 104 broadcast
R1(config-if)#int lo0
R1(config-if)#ip add 1.1.1.1 255.255.255.0
```

封装帧中继。

关闭反向 ARP，取消自动 IP 地址到 DLCI 的自动映射功能。如果开启自动学习功能，R3 和 R4 间将使用一条不允许使用的 PVC。

使 R1 可以 ping 通本端。

因为取消反向 ARP 的自动学习功能，这里需要静态配置 IP 地址到 DLCI 的映射关系。

因为取消反向 ARP 的自动学习功能，这里需要静态配置 IP 地址到 DLCI 的映射关系。

R3 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#encapsulation frame-relay
R3(config-if)#no frame-relay inverse-arp
R3(config-if)#ip add 134.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#frame-relay map ip 134.1.1.1 301 broadcast
R3(config-if)#frame-relay map ip 134.1.1.3 301 broadcast
R3(config-if)#frame-relay map ip 134.1.1.4 301 broadcast
R3(config-if)#int lo0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
```

使 R3 可以 ping 通本端。

这里配置到 R4 IP 地址的 DLCI 号，因为 R3 和 R4 间并没有申请 PVC，这里是不允许使用 PVC 的，那么 R3 到 R4 要先发到 R1，然后由 R1 转发到 R4，所以 R3 把 R4 的 IP 地址和到 R1 的 DLCI 做映射。

R4 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R4
R4(config)#int s1/0
R4(config-if)#enca frame-relay
R4(config-if)#no frame-relay inverse-arp
R4(config-if)#ip add 134.1.1.4 255.255.255.0
R4(config-if)#no shut
R4(config-if)#frame-relay map ip 134.1.1.1 401 broadcast
R4(config-if)#frame-relay map ip 134.1.1.3 401 broadcast
R4(config-if)#frame-relay map ip 134.1.1.4 401 broadcast
R4(config-if)#int lo0
R4(config-if)#ip add 4.4.4.4 255.255.255.0
```

配置完帧中继后，R1、R3 和 R4 都可以 ping 通所有的 134.1.0/24 的地址。

接下来配置 RIP 路由协议。R1 的配置如下：

```
R1(config)#router rip
R1(config-router)#net 1.0.0.0
R1(config-router)#net 134.1.0.0
```

134 是 B 类地址，所以主类网络号是 134.1.0.0。

R3 的配置如下：

```
R3(config)#router rip
R3(config-router)#net 3.0.0.0
R3(config-router)#net 134.1.0.0
```

R4 的配置如下:

```
R4(config)#router rip
R4(config-router)#net 4.0.0.0
R4(config-router)#net 134.1.0.0
```

配置完成后, 稍候查看 R1 的路由表, 显示如下:

```
R1#show ip route
 1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, Loopback0
R    3.0.0.0/8 [120/1] via 134.1.1.3, 00:00:09, Serial1/1
R    4.0.0.0/8 [120/1] via 134.1.1.4, 00:00:16, Serial1/1
 134.1.0.0/24 is subnetted, 1 subnets
C    134.1.1.0 is directly connected, Serial1/1
```

R1 学到整个网络中的所有路由, 在 R1 上 ping 3.3.3.3 和 ping 4.4.4.4 均可以 ping 通。查看 R3 的路由表, 显示如下:

```
R3#show ip route
R    1.0.0.0/8 [120/1] via 134.1.1.1, 00:00:16, Serial1/0
 3.0.0.0/24 is subnetted, 1 subnets
C    3.3.3.0 is directly connected, Loopback0
R    4.0.0.0/8 [120/2] via 134.1.1.1, 00:00:16, Serial1/0
 134.1.0.0/24 is subnetted, 1 subnets
C    134.1.1.0 is directly connected, Serial1/0
```

从上面的输出中可以看出, R3 也学到了 R1 上的环回接口路由和 R4 上的环回接口路由。注意 4.0.0.0/8 的下一跳是 134.1.1.1, 也就是说, R3 到 4.0.0.0/8 网络的数据包的下一跳是 R1, 然后再由 R1 发往 R4。

R4 的路由表与 R3 类似, R4 去往 3.0.0.0/8 网络的数据包的下一跳是 R1, 然后再由 R1 发往 R3。

路由可达性问题

从上面的输出中, 并没有遇到上一节中提到的路由可达性问题, R3 发往 R1 S1/1 接口的路由, 又被 R1 从 S1/1 接口发往 R4。同样, R4 发往 R1 S1/1 接口的路由, 又被 R1 从 S1/1 接口发往 R3。出现这种现象, 是因为帧中继物理接口默认关闭了水平分割, 查看 R1 S1/1 接口的水平分割情况, 显示如下:

```
R1#show ip int s1/1
Serial1/1 is up, line protocol is up
 Internet address is 134.1.1.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.9
 Outgoing access list is not set
 Inbound access list is not set
 Proxy ARP is enabled
 Local Proxy ARP is disabled
 Security level is default
 Split horizon is disabled
后面无关的部分省略。
```

使用下面的命令打开 R1 S1/1 接口的水平分割:

```
R1(config)#int s1/1
R1(config-if)#ip split-horizon
```

使用 “clear ip route *” 命令, 清除 R3 和 R4 的路由表, 让它们重新学习路由。然后查

看 R3 的路由表，显示如下：

```
R3#show ip route
R   1.0.0.0/8 [120/1] via 134.1.1.1, 00:00:12, Serial1/0
    3.0.0.0/24 is subnetted, 1 subnets
C    3.3.3.0 is directly connected, Loopback0
    134.1.0.0/24 is subnetted, 1 subnets
C    134.1.1.0 is directly connected, Serial1/0
```

从上面的输出中，可以看到水平分割已经发生作用了，R1 不再把从 S1/1 接口学到的 4.0.0.0/8 的路由从同一个接口再发出去，R3 学不到 R4 上环回接口的路由。同理，R4 也学不到 R3 上环回接口的路由。解决的办法之一就是前面使用的关闭水平分割；办法之二就是接下来要介绍的使用点到点接口。

16.2.3 帧中继接口**

上一节提到子接口有两种连接类型：点到点 (Point-to-Point) 和多点子接口 (Multipoint)。本小节介绍这两种类型子接口的配置。

帧中继多点子接口的配置与物理接口的配置类似，如果帧中继的一个多点子接口同时连接到多个路由器的物理接口或子接口，所有的接口配置在同一个子网中，此时如果没有全互连，这将和帧中继物理接口一样，如果启用水平分割，也会导致路由可达性问题。

在图 16-2-3 中，路由器 R1 使用 S1/1.2 多点子接口同时连接到 R3 和 R4，R1 的 S1/1.2 多点子接口的 IP 地址是 134.1.1.1/24，R3 的 S1/0 接口的 IP 地址是 134.1.1.3/24，R4 的 S1/0 接口的 IP 地址是 134.1.1.4/24。这 3 个接口的 IP 地址同属于一个子网。

帧中继的点到点接口配置中，每一个点到点接口只连接到一台路由器的物理接口或子接口，路由器的多个点到点接口分属于不同的子网，此时不论多台路由器之间是否全互连，接口是否启用水平分割，都不会存在路由可达性问题。

在图 16-2-3 中，路由器 R1 使用 S1/1.1 点到点接口连接 R2，点到点接口只能连接一台设备。R1 S1/1.1 和 R1 S1/1.2 是 R1 上的不同子接口，配置的 IP 地址属于不同的子网。R1 S1/1.1 点到点接口的 IP 地址是 12.1.1.1/24，R2 S1/0 接口的 IP 地址是 12.1.1.2/24。这两个接口属于同一个子网，是一条点到点的链路。

Dynamips CCNA 机架上的 R2 要模拟帧中继交换机，因此该实验台只能完成三台帧中继路由器的实验，实验拓扑如图 16-2-4 所示。图中 R1 使用 S1/1.1 点到点接口与 R3 相连，该子接口的 IP 地址是 13.1.1.1/24，R3 S1/0 接口的 IP 地址是 13.1.1.3/24。R1 使用 S1/1.2 多点子接口与 R4 相连，尽管 R1 的 S1/1.2 子接口只连接到 R4 一台路由器，更适合使用点到点接口类型，这里使用多点子接口，仅仅是为了说明多点子接口的配置，R1 S1/1.2 多点子接口的 IP 地址是 14.1.1.1/24，R4 S1/0 接口的 IP 地址是 14.1.1.4/24。

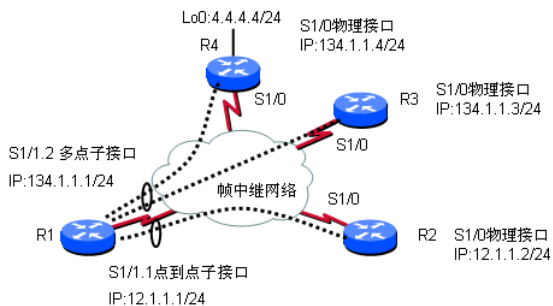


图 16-2-3 帧中继接口类型

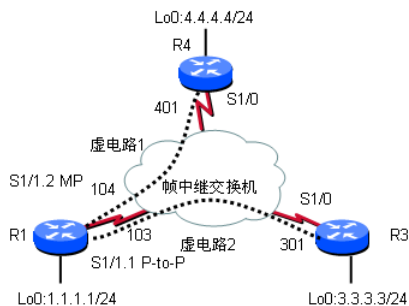


图 16-2-4 帧中继接口实验

路由器 R1 配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#encapsulation frame-relay
R1(config-if)#no frame-relay inverse-arp
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#int s1/1.1 ?
    multipoint      Treat as a multipoint link
    point-to-point  Treat as a point-to-point link

R1(config)#int s1/1.1 point-to-point
R1(config-subif)#ip add 13.1.1.1 255.255.255.0
R1(config-subif)#frame-relay interface-dlci 103
R1(config-fr-dlci)#exit
R1(config-subif)#exit
R1(config)#int s1/1.2 multipoint
R1(config-subif)#ip add 14.1.1.1 255.255.255.0
R1(config-subif)#frame-relay map ip 14.1.1.1 104 broadcast
R1(config-subif)#exit
R1(config)#int lo0
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config-if)#router rip
R1(config-router)#net 1.0.0.0
R1(config-router)#net 13.0.0.0
R1(config-router)#net 14.0.0.0
```

配置帧中继的物理接口。
给物理接口封装帧中继。
关闭反向 ARP。
和单臂路由一样，使用子接口，物理接口也要打开。
使用在线帮助，可以发现第一次进帧中继的子接口，必须要指明该子接口的类型是多点子接口还是点到点子接口。
S1/1.1 是一个点到点子接口。
点到点子接口不需要映射 IP 地址到 DLCI，只需要指明该接口使用的 DLCI 号就可以了。点到点子接口也不需要映射本端的 IP 地址，点到点子接口去往该子接口 IP 地址和远端路由器 IP 地址的数据帧，都用点到点子接口的 DLCI 号封装。
S1/1.2 是一个多点子接口。
S1/1.1 和 S1/1.2 是 R1 上不同的子接口，路由器的不同接口需要配置不同子网的 IP 地址。
多点子接口与物理接口类似，在关闭反向 ARP 的情况下，需要配置 IP 地址到 DLCI 号的映射。如果需要 ping 通本端，路由器本端的 IP 地址也需要静态映射。
配置 RIP 协议。

路由器 R3 配置如下：

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#enca frame-relay
R3(config-if)#no fram inverse-arp
R3(config-if)#ip add 13.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#frame-relay map ip 13.1.1.1 301 broadcast
R3(config-if)#frame-relay map ip 13.1.1.3 301 broadcast
R3(config-if)#int lo0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
R3(config-if)#router rip
R3(config-router)#net 3.0.0.0
R3(config-router)#net 13.0.0.0
```

路由器 R4 配置如下：

```
Router>en
Router#conf t
Router(config)#host R4
R4(config)#int s1/0
R4(config-if)#enca frame-relay
R4(config-if)#no fram inver
R4(config-if)#ip add 14.1.1.4 255.255.255.0
R4(config-if)#no shut
```



```
R4(config-if)#frame-relay map ip 14.1.1.1 401 broadcast
R4(config-if)#frame-relay map ip 14.1.1.4 401 broadcast
R4(config-if)#int lo0
R4(config-if)#ip add 4.4.4.4 255.255.255.0
R4(config-if)#router rip
R4(config-router)#net 4.0.0.0
R4(config-router)#net 14.0.0.0
```

配置完成后，查看 R1 的路由表，显示如下：

```
R1#show ip route
 1.0.0.0/24 is subnetted, 1 subnets
 C    1.1.1.0 is directly connected, Loopback0
R   3.0.0.0/8 [120/1] via 13.1.1.3, 00:00:12, Serial1/1.1
R   4.0.0.0/8 [120/1] via 14.1.1.4, 00:00:17, Serial1/1.2
 13.0.0.0/24 is subnetted, 1 subnets
 C    13.1.1.0 is directly connected, Serial1/1.1
 14.0.0.0/24 is subnetted, 1 subnets
 C    14.1.1.0 is directly connected, Serial1/1.2
```

从上面的输出中可以看到，R1 学到了所有网络的路由条目。在 R1 上 ping 13.1.1.1、13.1.1.3、14.1.1.1、14.1.1.4、1.1.1.1、3.3.3.3、4.4.4.4，均可以 ping 通。

查看 R3 的路由表，显示如下：

```
R3# show ip route
R   1.0.0.0/8 [120/1] via 13.1.1.1, 00:00:25, Serial1/0
 3.0.0.0/24 is subnetted, 1 subnets
 C    3.3.3.0 is directly connected, Loopback0
R   4.0.0.0/8 [120/2] via 13.1.1.1, 00:00:25, Serial1/0
 13.0.0.0/24 is subnetted, 1 subnets
 C    13.1.1.0 is directly connected, Serial1/0
R   14.0.0.0/8 [120/1] via 13.1.1.1, 00:00:25, Serial1/0
```

从上面的输出中可以看到，R3 学到了所有网络的路由条目。R3 去往 4.0.0.0/8 的路由有两跳，即先到 R1 再到 R3。还记得在前面 16.2.2 节的配置中，R3 去往 R4 上环回接口的路由也是发给 R1，都经过 2 跳。在 R3 上 ping 13.1.1.1、13.1.1.3、14.1.1.1、14.1.1.4、1.1.1.1、3.3.3.3、4.4.4.4，均可以 ping 通。

查看 R4 的路由表，显示如下：

```
R4#show ip route
R   1.0.0.0/8 [120/1] via 14.1.1.1, 00:00:15, Serial1/0
R   3.0.0.0/8 [120/2] via 14.1.1.1, 00:00:15, Serial1/0
 4.0.0.0/24 is subnetted, 1 subnets
 C    4.4.4.0 is directly connected, Loopback0
R   13.0.0.0/8 [120/1] via 14.1.1.1, 00:00:15, Serial1/0
 14.0.0.0/24 is subnetted, 1 subnets
 C    14.1.1.0 is directly connected, Serial1/0
```

从上面的输出中可以看到，R4 学到了所有网络的路由条目。在 R4 上 ping 13.1.1.1、13.1.1.3、14.1.1.1、14.1.1.4、1.1.1.1、3.3.3.3、4.4.4.4，均可以 ping 通。

可以看出 R3 和 R4 都学到了彼此之间的路由，查看 R1 上两个子接口水平分割的使用情况，显示如下：

```
R1#show ip int s1/1.1
Serial1/1.1 is up, line protocol is up
 Internet address is 13.1.1.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.9
 Outgoing access list is not set
```

```
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled

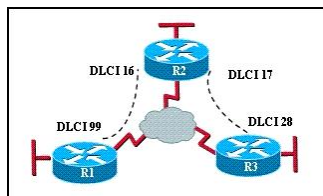
R1#show ip int s1/1.2
Serial1/1.2 is up, line protocol is up
Internet address is 14.1.1.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.9
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
```

从上面的输出中，可以看到帧中继的点到点子接口和多点子接口，水平分割默认都是打开的，但这里并没有影响 R3 和 R4 路由的传递，这是因为 R3 和 R4 分别连接 R1 的不同子接口，水平分割对不同子接口路由传入和传出不起作用。这里要提醒的是，如果 R1 的 S1/1.2 多点子接口同时连接到多台路由器，远程路由器之间学习路由要受到水平分割的影响。



16.3 真题精选***

1. Refer to the exhibit. Which statement describes DLCI 17?



- A. DLCI 17 describes the ISDN circuit between R2 and R3.
- B. DLCI 17 describes a PVC on R2. It cannot be used on R3 or R1.
- C. DLCI 17 is the Layer 2 address used by R2 to describe a PVC to R3.
- D. DLCI 17 describes the dial-up circuit from R2 and R3 to the service provider.

2. Refer to the exhibit. Which two statements are true based the output of the show frame-relay lmi command issued on the Branch router? (Choose two.)

```
Branch# show frame-relay lmi
LMI Statistics for interface Serial0/0 (Frame Relay DTE) LMI TYPE = ANSI
Invalid Unnumbered info 0      Invalid Prot Disc 0
Invalid dummy Call Ref 0      Invalid Msg Type 0
Invalid Status Message 0      Invalid Lock Shift 0
Invalid Information ID 0       Invalid Report IE Len 0
Invalid Report Request 0       Invalid Keep IE Len 0
Num Status Enq. Sent 61        Num Status msgs Rcvd 0
Num Update Status Rcvd 0       Num Status Timeouts 60
Branch#
```

- A. LMI messages are being sent on DLCI 0.
- B. LMI messages are being sent on DLCI 1023.

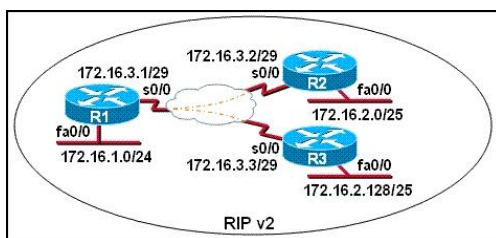
- C. Interface Serial0/0 is not configured to encapsulate Frame Relay.
- D. The Frame Relay switch is not responding to LMI requests from the router.
- E. The LMI exchange between the router and Frame Relay switch is functioning properly.
- F. The router is providing a clock signal on Serial0/0 on the circuit to the Frame Relay switch.

3. Refer to the exhibit. What is the meaning of the term dynamic as displayed in the output of the show frame-relay map command shown?

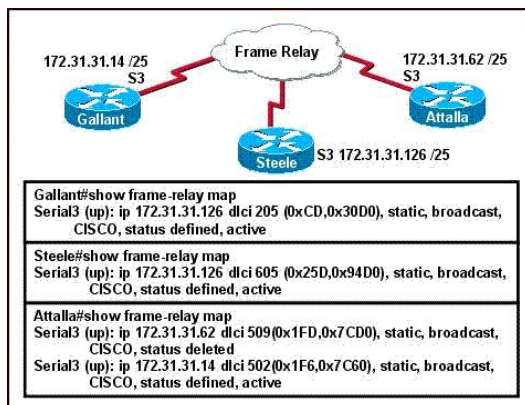
```
R1# show frame-relay map
Serial0/0 (up): ip 172.16.3.1 dlci 100 (0x64, 0x1840), dynamic
broadcast, status defined, active
```

- A. The Serial0/0 interface is passing traffic.
 - B. The DLCI 100 was dynamically allocated by the router.
 - C. The Serial0/0 interface acquired the IP address of 172.16.3.1 from a DHCP server.
 - D. The DLCI 100 will be dynamically changed as required to adapt to changes in the Frame Relay cloud.
 - E. The mapping between DLCI 100 and the end station IP address 172.16.3.1 was learned through Inverse ARP.
4. A default Frame Relay WAN is classified as what type of physical network?
- A. point-to-point
 - B. broadcast multi-access
 - C. nonbroadcast multi-access
 - D. nonbroadcast multipoint
 - E. broadcast point-to-multipoint
5. How should a router that is being used in a Frame Relay network be configured to avoid split horizon issues from preventing routing updates?
- A. Configure a separate sub-interface for each PVC with a unique DLCI and subnet assigned to the sub-interface.
 - B. Configure each Frame Relay circuit as a point-to-point line to support multicast and broadcast traffic.
 - C. Configure many sub-interfaces on the same subnet.
 - D. Configure a single sub-interface to establish multiple PVC connections to multiple remote router interfaces.
6. The command frame-relay map ip 10.121.16.8 102 broadcast was entered on the router. Which of the following statements is true concerning this command?
- A. This command should be executed from the global configuration mode.
 - B. The IP address 10.121.16.8 is the local router port used to forward data.
 - C. 102 is the remote DLCI that will receive the information.
 - D. This command is required for all Frame Relay configurations.
 - E. The broadcast option allows packets, such as RIP updates, to be forwarded across the PVC.
7. Refer to the exhibit. S0/0 on R1 is configured as a multipoint interface to communicate with R2 and R3 in this hub-and-spoke Frame Relay topology. While testing this configuration, a technician notes that pings are successful from hosts on the 172.16.1.0/24 network to hosts on both the 172.16.2.0/25 and 172.16.2.128/25 networks.

However, pings between hosts on the 172.16.2.0/25 and 172.16.2.128/25 networks are not successful. What could explain this connectivity problem?

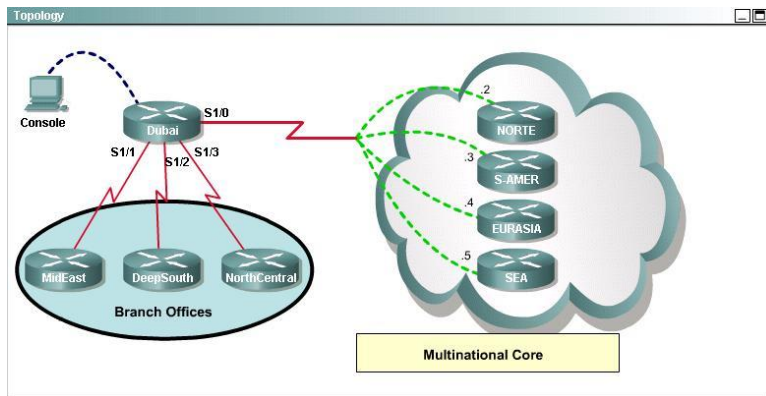


- A. The ip subnet-zero command has been issued on the R1 router.
 - B. The RIP v2 dynamic routing protocol cannot be used across a Frame Relay network.
 - C. Split horizon is preventing R2 from learning about the R3 networks and R3 from learning about the R2 networks.
 - D. The 172.16.2.0/25 and 172.16.2.128/25 networks are overlapping networks that can be seen by R1, but not between R2 and R3.
 - E. The 172.16.3.0/29 network used on the Frame Relay links is creating a discontinuous network between the R2 and R3 router subnetworks.
8. The Frame Relay network in the diagram is not functioning properly. What is the cause of the problem?



- A. The Gallant router has the wrong LMI type configured.
 - B. Inverse ARP is providing the wrong PVC information to the Gallant router.
 - C. The S3 interface of the Steele router has been configured with the frame-relay encapsulation ietf command.
 - D. The frame-relay map statement in the Attalla router for the PVC to Steele is not correct.
 - E. The IP address on the serial interface of the Attalla router is configured incorrectly.
9. A Cisco router that was providing Frame Relay connectivity at a remote site was replaced with a different vendor's frame relay router. Connectivity is now down between the central and remote site. What is the most likely cause of the problem?
- A. mismatched LMI types
 - B. incorrect DLCI
 - C. mismatched encapsulation types
 - D. incorrect IP address mapping

10. Hotspot:



```

Dubai#sh frame-relay map
Serial1/0 (up): ip 172.30.0.2 dlci 704 (0x7B,0x1CB0),dynamic,
                broadcast,,status defined,active
Serial1/0 (up): ip 172.30.0.3 dlci 196 (0xEA,0x38A0),dynamic,
                broadcast,,status defined,active
Serial1/0 (up): ip 172.30.0.4 dlci 702 (0x159,0x5490),dynamic,
                broadcast,,status defined,active
Serial1/0 (up): ip 172.30.0.5 dlci 344 (0x1C8,0x7080),dynamic,
                broadcast,,status defined,active

Dubai#
interface FastEthernet0/0
no ip address
shutdown
!
interface Serial1/0
ip address 172.30.0.1 255.255.255.240
encapsulation frame-relay
no fair-queue
!
interface Serial1/1
ip address 192.168.0.1 255.255.255.252
!
interface Serial1/2
ip address 192.168.0.5 255 255 255 252
encapsulation ppp
!
interface Serial1/3
ip address 192.168.0.9 255.255.255.252
encapsulation ppp
ppp authentication chap
!
router rip
version 2
network 172.30.0.0
network 192.168.0.0
no auto-summary
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0
password Tlnet
login
!
end

```

<p>Question #1</p> <p>What destination Layer 2 address will be used in the frame header containing a packet for host 172.30.4.4?</p> <p><input type="radio"/> 704</p> <p><input type="radio"/> 196</p> <p><input type="radio"/> 702</p> <p><input type="radio"/> 344</p>	<p>Question #3</p> <p>Which connection uses the default encapsulation for serial interfaces on Cisco routers?</p> <p><input type="radio"/> The serial connection to the MidEast branch office.</p> <p><input type="radio"/> The serial connection to the DeepSouth branch office.</p> <p><input type="radio"/> The serial connection to the NorthCentral branch office.</p> <p><input type="radio"/> The serial connection to the Multinational Core.</p>
<p>Question #2</p> <p>A static map to the S-AMER location is required. Which command should be used to create this map?</p> <p><input type="radio"/> frame-relay map ip 172.30.0.3 704 broadcast</p> <p><input type="radio"/> frame-relay map ip 172.30.0.3 196 broadcast</p> <p><input type="radio"/> frame-relay map ip 172.30.0.3 702 broadcast</p> <p><input type="radio"/> frame-relay map ip 172.30.0.3 344 broadcast</p>	<p>Question #4</p> <p>If required, what password should be configured on the router in the MidEast branch office to allow a connection to be established with the Dubai router?</p> <p><input type="radio"/> No password is required.</p> <p><input type="radio"/> En8ble</p> <p><input type="radio"/> Scr8</p> <p><input type="radio"/> T1net</p> <p><input type="radio"/> C0nsole</p>

Hotspot question. Click on the correct location or locations in the exhibit.



16.4 真题解答***

1. 解：C

题目问：参照图，哪一个语句描述了 DLCI 17？DLCI 是 Frame Relay 中描述的二层地址信息，对于 R2 来说，DLCI 17 可以到达 R3，图中 R2 上的 DLCI 17 和 R3 上的 DLCI 28 组成了一条 PVC（永久虚电路）。

2. 解：AD

题目问：参照图，基于在 Branch 路由器上“show frame-relay lmi”命令的输出，哪两个语句是正确的？参照本章 16.1.2 节，从图中可以看到帧中继 LMI 的类型是 ANSI，部分 DLCI 被保留用于特殊的用途，比如 DLCI=0 表示 ANSI 和 Q933A 定义的 LMI，而 DLCI=1023 表示 Cisco 定义的 LMI；“Num Status msgs Rcvd 0”表示收到的 LMI 消息是 0 个，也就是没有收到 LMI 消息，表明帧中继交换机没有响应路由器的查询。

3. 解：E

题目问：参照图，“show frame-relay map”命令输出中的“dynamic”是什么意思？参照本章 16.1.4 节，这是个关于帧中继映射的问题，在图中可以看到这个 MAP 是 dynamic（动态）的，因此是通过反向（inverse）ARP 学习到的。而“ip 172.16.3.1 dlci 100”表示 DLCI 100 映射的 IP 地址是 172.16.3.1。

4. 解：C

题目问：默认的帧中继广域网被认为是什么类型的物理网络？参照本章 16.1.4 节，在默认的情况下，帧中继为 NBMA（Non-Broadcast Multiple Access，非广播多路访问）的网络，通过发送帧的多个拷贝来解决广播问题，每个帧被封装了不同的 DLCI 号来到达不同的目的端。

5. 解：A

题目问：怎样配置帧中继网络中的路由器来避免水平分割阻止路由更新的问题？参照本章 16.1.5 节，解决水平分割产生的路由更新可达性问题，可以使用两种方法，方法一是关闭水平分割；方法二是使用多个点对点的子接口，每个子接口都有单独的 DLCI 号，把每个子接口分配到不同的 IP 子网中。

6. 解: E

题目问: 在路由器上输入 “frame-relay map ip 10.121.16.8 102 broadcast” 命令, 关于这条命令下面哪一个语句是正确的? 参照本章 16.2.1 节, 这条命令是接口配置命令, 手工静态添加一条映射, 到达 10.121.16.8 的流量封装一个 DLCI 号为 102, 而且这条 PVC 可以支持广播流量, 比如 RIP 的更新包。因为在默认的情况下, 帧中继的网络为非广播的, 而 RIP 在其上是无法发送的。

7. 解: C

题目问: 参照图, 在 Hub-and-Spoke 拓扑中, R1 的 S0/0 被配置成多点子接口与 R2 和 R3 通信, 从 172.16.1.0/24 子网中的主机可以成功地 ping 通 172.16.2.0/25 和 172.16.2.128/25 子网中的主机, 但 172.16.2.0/25 和 172.16.2.128/25 子网中的主机相互之间 ping 失败, 可能是什么样的连接问题? 根据本章的介绍, 该题是水平分割与路由的可达性问题, 与 16.2.2 节的叙述现象相同。在帧中继的环境中, 在默认情况下, 物理接口的水平分割是关闭的, 如果打开水平分割则会造成 Spoke 端相互间学不到对方的路由, 但 Hub 端可以学到所有 Spoke 端的路由; 图中如果使用的是多点子接口, 可以参照 16.2.3 节, 在帧中继的环境中, 在默认情况下, 子接口的水平分割是打开的, 也会造成 Spoke 端相互间学不到对方的路由。本题目是由于 R1 的 S0/0 接口的水平分割阻止了 R2 和 R3 之间相互学习对方的路由。

8. 解: D

题目问: 图中的帧中继网络工作不正常, 导致的原因是什么? 可以参照本章 16.2.1 节, 从输出中可以看到这是一个 NBMA 网络, 图中没有给出具体的 PVC, 根据图中的输出, 可以猜想初衷应该是配置 Hub-and-Spoke 拓扑, 打算静态配置 Gallant 到 Attalla 和 Steele 到 Attalla 两条 PVC。Gallant 和 Attalla 之间的 PVC, Attalla 配置的都正确, 但 Gallant 却映射成 Steele 的地址; Steele 和 Attalla 之间的 PVC 配置错误, 静态映射中都没有映射对方的 IP 地址, 而是映射了本地的 IP 地址。由于图中没有给出具体的 PVC, 本题最好的方法是使用排除法, 排除所有说法错误的选项。A 选项说 Gallant 配置的 LMI 类型有错, 从图中看不出这一点; B 选项说反向 ARP 给 Gallant 路由器提供了错误的 PVC 信息, 从图中可以看到, 网络中并没有使用反向 ARP, 所有的映射都是静态配置的; C 选项说 Steele 的 S3 帧中继的封装类型是 ietf, 从 “Steele 上 show frame-relay map” 命令的输出中, 可以清楚地看到封装的类型是 Cisco; E 选项说 Attalla 路由器串行接口的 IP 地址配置错误, 172.31.31.62/25 既不是子网地址也不是子网广播, 是一个合法的 IP 地址。D 选项的描述虽不全面, 却是错误的一部分。综上所述, D 是正确答案。

9. 解: C

题目问: 一台思科路由器在远程站点提供帧中继的连接, 思科路由器被不同厂商的帧中继路由器替换后, 中心站点和远程站点的连接中断, 最可能导致问题的原因是什么? 不匹配的 LMI 类型会导致远程站点与帧中继交换机之间连接失败, 进而导致与中心站点连接失败; 不正确的 DLCI 配置也会导致连接失败; 不正确的 IP 地址映射也会导致连接失败; 但根据题中所述, 最可能的却是封装类型不一致, 思科路由器默认的帧中继封装类型是 Cisco, 其他厂商的帧中继封装只有 IETF, 两端的帧中继封装类型不一致, 连接失败, 解决的办法是更改中心站点的帧中继封装类型为 IETF。

10. 解

第一个问题问的是，Dubai 路由器上有一个包要去往主机 172.30.4.4（题中有错，应该是 172.30.0.4），第二层帧头中使用的目标地址是什么？根据“show frame-relay map”命令输出中显示的映射，要去往 172.30.0.4，映射的 DLCI 号应该是 702。

第二个问题问的是，需要配置到 S-AMER 的静态映射，哪一个命令能创建这个映射？S-AMER 路由器的 IP 地址是 172.30.0.3，从“show frame-relay map”命令输出中可以看到对应的 DLCI 号是 196，正确的命令应该是“frame-relay map ip 172.30.0.3 196 broadcast”。

第三个问题问的是，哪一个连接使用了思科路由器串行接口的默认封装？思科路由器串行接口的默认封装是 HDLC，从 Dubai 路由器的配置中，可以看到只有 S1/1 接口没有被配置封装协议，S1/1 接口连接的路由器是分支办公室中的 MidEast 路由器。

第四个问题问的是，如果需要，为了与 Dubai 路由器建立连接，什么密码将被配置在分支办公室的 MidEast 路由器上？从配置中可以看到 Dubai 与 MidEast 路由器之间的串行线路使用的是 HDLC 封装协议，该协议不支持验证，什么密码也不需要。

选择的答案如下：

<p>Question #1</p> <p>What destination Layer 2 address will be used in the frame header containing a packet for host 172.30.4.4?</p> <p> <input type="radio"/> 704 <input type="radio"/> 196 <input checked="" type="radio"/> 702 <input type="radio"/> 344 </p>	<p>Question #3</p> <p>Which connection uses the default encapsulation for serial interfaces on Cisco routers?</p> <p> <input checked="" type="radio"/> The serial connection to the MidEast branch office. <input type="radio"/> The serial connection to the DeepSouth branch office. <input type="radio"/> The serial connection to the NorthCentral branch office. <input type="radio"/> The serial connection to the Multinational Core. </p>
<p>Question #2</p> <p>A static map to the S-AMER location is required. Which command should be used to create this map?</p> <p> <input type="radio"/> frame-relay map ip 172.30.0.3 704 broadcast <input checked="" type="radio"/> frame-relay map ip 172.30.0.3 196 broadcast <input type="radio"/> frame-relay map ip 172.30.0.3 702 broadcast <input type="radio"/> frame-relay map ip 172.30.0.3 344 broadcast </p>	<p>Question #4</p> <p>If required, what password should be configured on the router in the MidEast branch office to allow a connection to be established with the Dubai router?</p> <p> <input checked="" type="radio"/> No password is required. <input type="radio"/> Enable <input type="radio"/> Scr8 <input type="radio"/> T1net <input type="radio"/> C0nsole </p>

第 17 章

访问控制列表***

本章介绍访问控制列表的作用，标准、扩展、命名访问控制列表的配置，配置访问控制列表有哪些注意事项。一些高级访问控制列表的配置，包括动态、反射和基于时间访问控制列表等。



17.1 ACL 概述**

本节介绍 ACL 定义、ACL 作用、ACL 工作流程等。

17.1.1 ACL 定义**

ACL（Access Control List，访问控制列表）是一系列运用到路由器接口的指令列表。这些指令告诉路由器接收哪些数据包、拒绝哪些数据包，接收或者拒绝根据一定的规则进行，如源地址、目标地址、端口号等。ACL 使得用户能够管理数据流，检测特定的数据包。

路由器将根据 ACL 中指定的条件，对经过路由器端口的数据包进行检查。ACL 可以基于所有的 Routed Protocols（被路由协议，如 IP、IPX 等）对经过路由器的数据包进行过滤。ACL 在路由器的端口过滤数据流，决定是否转发或者阻止数据包。ACL 应该根据路由器的端口所允许的每个协议来制定，如果需要控制流经某个端口的所有数据流，就需要为该端口允许的每一个协议分别创建 ACL。例如，如果端口被配置为允许 IP、AppleTalk 和 IPX 协议的数据流，那么就需要创建至少 3 个 ACL，CCNA 课程中仅讨论 IP 的访问控制列表。针对 IP 协议，在路由器的每一个端口，可以创建两个 ACL：一个用于过滤进入（inbound）端口的数据流，另一个用于过滤流出（outbound）端口的数据流。

一个 ACL 列表中可以包含多个 ACL 指令，ACL 指令的放置顺序很重要。当路由器在决定是否转发或者阻止数据包的时候，Cisco 的 IOS 软件，按照 ACL 中指令的顺序依次检查数据包是否满足某一个指令条件。当检测到某个指令条件满足的时候，就执行该指令规定的动作，并且不会再检测后面的指令条件。

17.1.2 ACL 作用**

ACL 可以用做控制和过滤流经路由器端口的数据包的工具。通过使用 ACL，路由器提供了基本的数据流过滤能力。ACL 具有下列作用：

- **限制网络流量，提高网络性能。**例如：根据不同的协议，ACL 可以指定路由器优先处理哪些数据包，这叫做队列管理，路由器可以不处理不需要的数据包。队列管理限制了网络数据流，减少了网络拥塞。

- **提供数据流控制。**例如：ACL 可以限定或者减少路由更新的内容。这些限定，可以用于限制关于某个特定网络的信息传播到整个网络。
- **为网络访问提供基本的安全层。**ACL 可以允许某个主机访问网络的某一部分，而阻止另一台主机访问网络的这个部分。
- **决定转发或者阻止哪些类型的数据流。**例如：可以允许 E-mail 数据流，而阻止 Telnet 数据流。

17.1.3 ACL 工作流程***

无论是否使用 ACL，通信处理过程的开始都是一样的。如图 17-1-1 所示，当路由器的某个接口收到一个分组时，路由器首先检查该分组是否是可路由的，如果不可路由（比如并非是发往本路由器的数据报文，或是一个不可被路由的协议），路由器则丢弃该数据包。

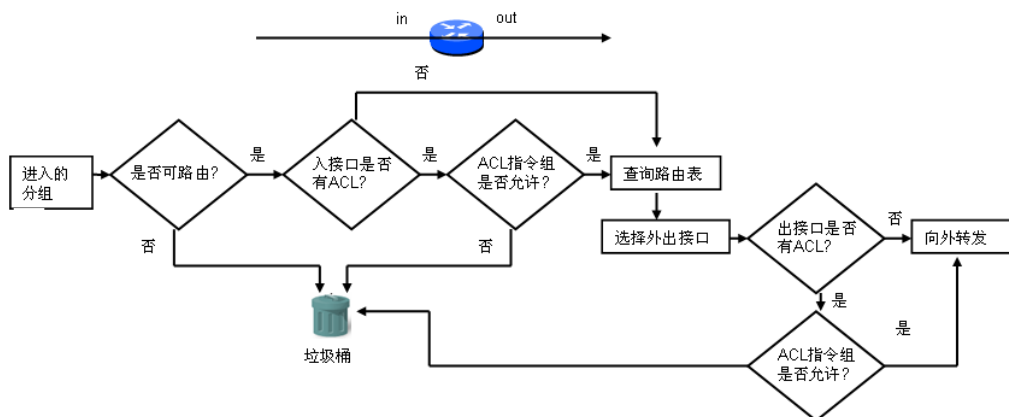


图 17-1-1 路由器上 ACL 的工作流程

接下来，路由器判断该入接口上有没有 ACL，如果没有则直接查询路由表；如果有 ACL，则判断该 ACL 的指令组是否允许该分组通过，如果不允许通过，则丢弃。如果 ACL 的指令组允许该分组通过，再查询路由表。从这里可以看出在路由器的入站方向，ACL 检测在查询路由表前被执行，这也是合理的，免得先查询路由表，结果还要被丢弃，白白浪费查询时间。

路由器查询路由表，选择该分组的外出接口。检测外出接口是否有 ACL，如果没有 ACL，则转发分组；如果外出接口也有 ACL，则判断 ACL 指令组是否允许该分组通过，如果允许，则向外转发；如果拒绝，则丢弃该分组。

上面提到了 ACL 指令组是允许还是拒绝。事实上，ACL 指令组可能会包含多个语句，ACL 指令组的执行过程如图 17-1-2 所示。

首先检查 ACL 指令组的第一条指令与收到的分组是否匹配。如果匹配，看该条指令规定的动作是允许还是拒绝，如果是允许，则转发该分组，

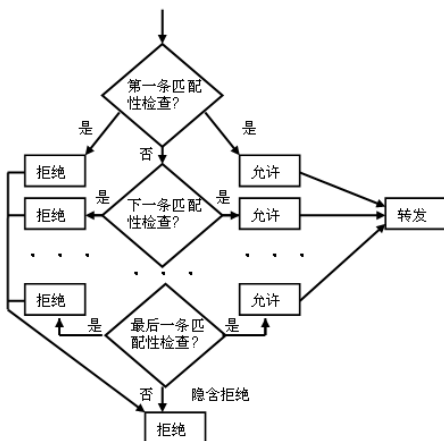


图 17-1-2 ACL 指令组的执行过程

如果是拒绝，则丢弃该分组，同时退出该 ACL 指令组，不再继续往下比较。如果不匹配，则执行第二条指令，这里的操作和第一条指令一样，如果匹配，则执行规定的动作，转发或丢弃，并退出该指令组的执行。如果第二条指令也不匹配，继续查找第三条指令，如果所有指令都不匹配，隐含的动作是拒绝。

17.1.4 ACL 类型**

ACL 根据功能不同，有多种类型，CCNA 中涉及的有标准 ACL、扩展 ACL、动态 ACL、自反 ACL 和基于时间的 ACL，本章后面会陆续介绍这几种 ACL 的使用。CCNA 考试的重点是标准 ACL 和扩展 ACL 的使用。



17.2 标准 ACL **

本节介绍标准 ACL 的创建、修改和应用，通配符掩码的使用，命名标准 ACL 的创建、修改和应用。

17.2.1 通配符掩码***

开始配置访问控制列表之前，必须掌握通配符掩码（Wildcard Masking）的作用和写法。路由器使用通配符掩码与源或目标地址一起来分辨匹配的地址范围。像子网掩码告诉路由器 IP 地址的哪些位属于网络号一样，通配符掩码告诉路由器为了判断匹配情况，它需要检查 IP 地址中的哪些位。IP 地址和通配符掩码一起来确定 IP 地址的范围，这是十分方便的，因为如果没有通配符掩码的话，不得不对每个匹配的 IP 地址加入一个单独的访问控制列表语句，这将造成很多额外的输入和路由器大量额外的处理过程，所以地址掩码对相当有用。

在子网掩码中，将掩码的一位设为 1 表示 IP 地址对应的位属于网络地址部分。而在访问控制列表中，将通配符掩码中的一位设为 1 表示忽略 IP 地址中对应的位，该位既可以是 1 又可以是 0，有时，可将其称做“不检查”位，因为路由器在判断是否匹配时并不关心它们。通配符掩码位设为 0 则表示 IP 地址中相对应的位必须精确匹配。下面看一些在访问控制列表中可能出现的地址掩码对是如何工作的。

192.168.1.0 0.0.0.255

通配符掩码是 0.0.0.255，前面是 24 个 0，最后是 8 个 1。通配符掩码中 0 表示必须精确匹配，也就是说，要精确匹配前面的 24 位。通配符掩码中 1 表示忽略位，随便是什么都可以，也就是说，最后的 8 位是 0 或 1 都没有关系。通配符掩码与前面的 IP 地址 192.168.1.0 结合在一起，实现的就是匹配从 192.168.1.0 到 192.168.1.255 的所有 IP 地址，即 192.168.1.* 的 IP 地址都满足这个地址对。

192.168.0.0 0.0.255.255

分析同上，实现的是匹配从 192.168.0.0 到 192.168.255.255 的所有 IP 地址，即 192.168.*.* 的 IP 地址都满足这个地址对。

并不是所有的通配符掩码的“精确匹配”位和“不检查”位都刚好是 8 的倍数。有时，计算什么匹配什么不匹配是十分困难的事。“192.168.16.0 0.0.7.255”地址和掩码对匹配的是哪些 IP 地址呢？

把地址和通配符掩码中的第三个十进制数进行二进制分解：

地址位：16=00010000

掩码位：7 =00000111

可以看出，如果不管通配符掩码中为 1 的相对应的地址位，IP 地址的最后 3 个比特任意取值，可以是 8 种可能的数字，从“000”到“111”，即从 16 到 23。整个的地址掩码对，实现的是匹配从 192.168.16.0 到 192.168.23.255 的所有 IP 地址。

“192.168.1.0 0.0.0.254”地址和通配符掩码实现的是匹配 192.168.1.0 网段中的所有偶数 IP 地址。“192.168.1.1 0.0.0.254”地址和通配符掩码实现的是匹配 192.168.1.0 网段中的所有奇数 IP 地址。注意到通配符掩码中二进制“1”出现的位置可以不连续，而子网掩码中“1”连续出现在前面的一些位，后面则是连续的“0”。

对于访问控制列表，判断是否匹配的过程实际分为 3 个步骤。在数据包过滤中，为进行匹配，路由器检查 IP 数据包报头中的 IP 地址。假设访问控制列表语句中包含地址掩码对 192.168.0.0 0.0.0.255，一个数据包中包含源 IP 地址 192.168.0.2，路由器将如下操作：

步骤 1：用访问控制列表语句中的通配符掩码和地址执行逻辑或(192.168.0.0 和 0.0.0.255 执行逻辑或)，该操作的结果为 192.168.0.255。

步骤 2：用访问控制列表语句中的通配符掩码和数据包报头中的 IP 地址执行逻辑或(192.168.0.2 和 0.0.0.255 执行逻辑或)，结果是 192.168.0.255。

步骤 3：将两个结果相减。如果两个结果相等，相减的结果精确为零，则匹配；如果相减的结果不为零，则不匹配，对下条语句重复执行上述 3 个步骤。

人为判断则没那么复杂，192.168.0.0 0.0.0.255 匹配的是 192.168.0.*的 IP 地址，192.168.0.2 刚好在这个地址范围内。

在 IP 访问控制列表地址掩码对中，有两个关键字可以用来省略一些输入。一个是“any”，它可用来代替地址掩码对 0.0.0.0 255.255.255.255。可以看出，该地址掩码对匹配任何的 IP 地址。

另一个是“host”，用来代替通配符掩码 0.0.0.0。比如要实现匹配 IP 地址 192.168.1.2，则可以写成 192.168.1.2 0.0.0.0，该语句等同于 host 192.168.1.2。在标准访问控制列表中，当通配掩码是 0.0.0.0 时会被自动省略，如果是 host 192.168.1.2，host 也会被省略。也就是说，如果没有通配符掩码，则表示该掩码是 0.0.0.0，仅匹配一个 IP 地址。在扩展访问控制列表中，通配符掩码 0.0.0.0 或 host 关键字不可以省略。

17.2.2 配置标准 ACL**

本章的实验在 Dynamips 的 CCNA 机架中完成，运行 R1、R2、R3 三台路由器，它们的 IP 地址分配如图 17-2-1 所示。

首先配置静态路由，保证全网的连通性。其中 R1 的配置如下：

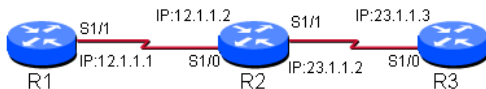


图 17-2-1 IP 地址分配

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#ip route 0.0.0.0 0.0.0.0 12.1.1.2
```

R2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
```

R3 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#ip route 0.0.0.0 0.0.0.0 23.1.1.2
```

静态路由配置完成后, R1 可以 ping 通 R3 的 S1/0 接口的 IP 地址 23.1.1.3, R2 也可以 ping 通 R3 的 S1/0 接口的 IP 地址 23.1.1.3。

接下来配置访问控制列表, 不允许 R1 访问 R3。配置访问控制列表分两个步骤: 创建 ACL 和应用 ACL。

1. 创建 ACL

访问控制列表是在全局配置模式下输入的。增加标准访问控制列表的基本格式如下:

```
access-list access-list-number {deny | permit} {source [source-wildcard] | any} [log]
```

参数 **access-list-number** 是 1 到 99 之间的整数, 是标准 ACL 的编号, 扩展 ACL 的编号从 100 到 199。然后规定是允许还是禁止从特定地址来的通信量, **deny** 是拒绝, 当来源 IP 地址匹配后面地址范围的时候, 流量将被丢弃; **permit** 是允许, 当来源 IP 地址匹配后面地址范围的时候, 流量将被允许。参数 **source** 指明了访问控制列表规则应用的源 IP 地址。如果想增加子网地址, 则可以把源地址从特定的主机变成一个 IP 地址范围。参数 **source-wildcard** 基本指明了地址字段中哪些位是匹配的。如果在末尾加上参数 **any**, 则表示地址 0.0.0.0 和通配符掩码 255.255.255.255, 这时所有的地址都是匹配的。**log** 是日志选项, 匹配的条目信息显示在控制台上, 也可以输出到日志服务器。

在路由器 R3 上创建访问控制列表, 配置如下:

```
R3 (config) #access-list 1 deny 12.1.1.1 拒绝 R1 的 IP 地址 12.1.1.1, 通配符掩码 0.0.0.0 可以省略。
R3 (config) #access-list 1 permit any
允许所有的 IP 地址, 这一行不能省略, 因为访问控制列表最后隐含了一条 deny any 的规则, 如果没有这一行, 所有的 IP 地址都将被拒绝。
```

上面两行的顺序很重要, 因为匹配的顺序是从上至下, 当条件匹配时即执行操作。如果把两行的顺序调换一下, 当 IP 地址 12.1.1.1 试图通过时, 12.1.1.1 是 **any** 中的一个地址, 执行的操作是允许, 永远执行不到第二条, 所有的 IP 地址都被允许, 这与要求不符。

2. 应用 ACL

创建好列表以后, 接下来还必须将它应用到每个想用它的接口。因为只想拒绝 R1 访问 R3, 其他的访问不受影响, 可以把列表用在 R3 的 S1/0 接口, 当数据包进入 R3 的时候进行

判断，配置如下：

```
R3 (config) #int s1/0
R3 (config-if) #ip access-group 1 in
```

在接口下调用访问控制列表 1，针对的是从 S1/0 接口进入路由器 R3 的流量。

至于是先创建列表，还是先在接口下调用列表，两个步骤的操作顺序没有关系，但两个步骤缺一不可，创建列表没有在接口下调用，或者在接口下调用一个没有被创建的列表，都不会起作用。配置完成后，在 R1 上 ping 23.1.1.3，ping 不通；在 R1 上 ping 12.1.1.2，可以 ping 通；在 R2 上 ping 23.1.1.3，也可以 ping 通。

17.2.3 编辑标准 ACL**

(1) 删除 ACL

ACL 配置完成后，如果不需要，可以使用命令删除 ACL。比如删除路由器 R3 上创建的 ACL 1，使用的命令如下：

```
R3 (config) #no access-list 1
```

删除某个 ACL，不需要输入具体的语句，只要删除该 ACL 对应的编号即可。

(2) 取消 ACL 在接口的应用

ACL 应用完成后，如果需要暂时解除 ACL 或者把 ACL 调整到其他接口，可以使用命令取消 ACL 在接口的应用。比如删除前面在 R3 S1/0 接口创建的 ACL，命令如下：

```
R3 (config) #int s1/0
R3 (config-if) #no ip access-group 1 in
```

(3) 编辑 ACL

ACL 配置完成后难免要进行编辑，如删除一行、插入一行等。因为标准 ACL 不能执行插入一行或删除一行的操作，推荐把现有的 ACL 拷贝到专门的文本编辑软件（如记事本等）中，对 ACL 进行编辑，然后删除路由器中的 ACL，再把编辑好的 ACL 粘贴到路由器的命令行窗口中。

17.2.4 标准 ACL 放置的位置***

列表写好以后，可以用在哪台设备、哪个接口、哪个方向上，还是有区别的。标准的访问控制列表只能针对源地址进行控制，把 12.1.1.1 作为源地址，R3 就成为目标地址了，数据流的方向就是从左到右，如图 17-2-2 所示。从 R1 到 R3，数据包共经过了 4 个接口，如果用在 R1 的 S1/1 接口，方向应该是 out；如果用在 R2 的 S1/0 接口，方向应该是 in；如果用在 R2 的 S1/1 接口，方向应该是 out；如果用在 R3 的 S1/0 接口，方向应该是 in。接下来分析把列表分别用在 4 个接口上有何不同，可以通过实验来验证下面的结论。

- 如果把前面创建的访问控制列表 1 配置在 R1 上，并在 R1 的 S1/1 接口调用，方向是 out。结果将不起作用，原因是访问控制列表仅对穿越路由器的数据包进行过滤，对本路由器起源的数据包不作过滤。这一点多数人都容易忽视，特别值得关注。
- 把前面创建的访问控制列表 1 配置在 R2 上，并在 R2 的 S1/0 接口调用，方向是 in。结果起作用，R1 不能访问 R3 了，可 R1

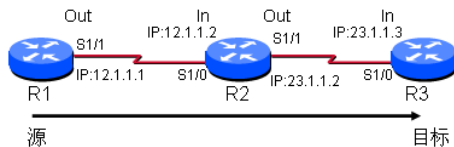


图 17-2-2 数据流的方向

也不能访问 R2 了，因为标准访问控制列表只能针对源地址，当 R1 访问 R2 的数据包进入路由器 R2 的 S1/0 接口时，源地址是 12.1.1.1 的数据包被丢弃，造成 R1 访问 R2 也失败。

- 如果用在 R2 的 S1/1 接口，方向是 out。结果正确。
- 如果用在 R3 的 S1/0 接口，方向是 in。结果也正确。

从上面的实验中可以得出结论，标准访问控制列表要尽量应用在靠近目标端，不然可能会带来错误影响，因为标准列表只能针对源地址进行过滤。

17.2.5 配置标准命名 ACL**

可以使用字符串代替数字，来标识 ACL，称为命名 ACL。使用命名 ACL 的优点包括：

- 可以在不删除整个 ACL 的情况下修改它。
- 用字符串可以更直观标识一个 ACL 的用途。
- 对于给定的协议，需要配置超出 99 个标准 ACL。

在使用命名 ACL 的时候，需要考虑到以下的因素：

- 命名 ACL 与 Cisco IOS 11.2 之前的版本不兼容。现在使用的 IOS 版本一般都是 12.0 以后的版本。
- 不能为多个 ACL 使用相同的名字。
- 不同类型的 ACL 不能使用相同的名字。例如，不能使用同一个名字来命名一个标准 ACL 和一个扩展 ACL。

使用下面的命令创建标准命名 ACL：

```
Router(config)# ip access-list standard access-list name
```

现在用标准命名 ACL 实现拒绝 R1 访问 R3，R3 的配置如下：

```
R3(config)#ip access-list standard deny-R1    创建标准命名 ACL deny-R1，这样字符的名字看起来更直观。
R3(config-std-nacl)#deny 12.1.1.1           拒绝主机 R1。
R3(config-std-nacl)#permit any               允许其他所有流量。
R3(config-std-nacl)#exit
R3(config)#int s1/0
R3(config-if)#ip access-group deny-R1 in      在接口下调用标准命名 ACL。
```

配置完成后，测试 R1 到 R3 的连通性，结果与使用标准编号 ACL 的效果相同。

标准命名 ACL 可以进行局部修改，在不删除整个 ACL 的情况下修改它。比如删除 deny 12.1.1.1 语句，则可以进行如下修改：

```
R3(config)#ip access-list standard deny-R1
R3(config-std-nacl)#no deny 12.1.1.1        删除标准命名 ACL 中的一行。
```

查看修改后的访问控制列表，显示如下：

```
R3#show access-lists
Standard IP access list 1
 10 deny 12.1.1.1(15 matches)
 20 permit any(30 matches)
Standard IP access list deny-R1
 20 permit any (15 matches)
```

注意到“(15 matches)”，表示有 15 个数据包满足该语句。前面的 20 是行号，在现在使用的多数 Cisco IOS 版本中，都支持这种行号显示。如果要删除“permit any”，也可以用下面的命令实现：

```
R3(config)#ip access-list standard deny-R1
R3(config-std-nacl)#no 20
```

删除行号将删除该行的内容。

在新版的 IOS 中，借鉴前面的方法，标准编号 ACL 也可以实现删除其中的某一行，执行如下：

```
R3(config)#ip access-list standard 1
R3(config-std-nacl)#no 10
```

编辑标准编号 ACL。
删除一行。

使用“show access-lists 1”命令查看 R3 上的访问控制列表，显示如下：

```
R3#show access-lists 1
Standard IP access list 1
 20 permit any (15 matches)
```

通过使用这种方法，标准编号 ACL 也可以实现在不删除整个 ACL 的情况下修改它。虽说这是多数思科交换机都支持的功能，可是 CCNA 考试并没有更新到新版 IOS，查看列表，将不会显示行号，在没有行号的情况下，针对行号的编辑工作将失败。

使用下面的命令删除标准命名 ACL：

```
R3(config)#no ip access-list standard deny-R1
```



17.3 扩展 ACL***

标准访问控制列表只能使用源地址作为过滤条件，提供了十分基本的过滤功能。扩展访问控制列表可以同时使用源地址和目标地址作为过滤条件，还可以针对不同的协议、协议的特征、端口号、时间范围等来过滤。扩展访问控制列表功能更强，可以更加细微地控制通信量。

17.3.1 配置扩展 ACL***

在匹配数据包时，扩展 IP 访问控制列表同时使用源地址和目标地址；还可以有选择地使用协议类型信息来优化控制，比如 TCP、UDP 协议及它们的端口号；也可以是时间参数，比如实现上班时间不可以上网，下班时间可以上网。许多在标准访问控制列表中使用的规则同样适用于扩展访问控制列表，配置扩展 ACL 也分为两个步骤：创建 ACL 和在接口下应用 ACL；在访问控制列表的结尾，隐式地拒绝所有等。

创建扩展 ACL 的基本格式如下：

```
access-list access-list-number {deny | permit | remark} protocol source [source-wildcard]
[operator operand] [port port-number or name] destination destination - wildcard [operator
operand] [port port-number or name] [established]
```

首先输入的是 access-list 命令，然后是访问控制列表的号码，号码的范围是 100~199，紧跟的参数是说明允许或者拒绝特定的通信量。remark 是注释，相当于在编写程序时，为了增加程序的可读性，人为添加的注释，注释的文本没有语法要求。然后需要指明将使用什么协议，如 TCP、UDP、ICMP 或者 IP。你可以告诉路由器明确的源地址和目标地址，也可以使用 any。如果是 TCP 或 UDP 还会涉及源端口和目标端口，如果是 ICMP 还会涉及包的类型，如 echo 或 echo-reply 等。established 是 TCP 协议中使用的一个关键字，意思是已建立，可以用来识别是不是 TCP 的初始连接。这里举一个使用扩展访问控制列表的例子。

针对图 17-2-1，拒绝 R1 去往 R3 的 Telnet 通信，允许其他的通信。在标准访问控制列表中，如果拒绝某个 IP 地址，就是拒绝该 IP 主机的所有服务，即拒绝 IP 整套协议；如果

允许某个 IP 地址，就是允许该 IP 主机的所有服务，即允许 IP 整套协议。如果只是拒绝 R1 去往 R3 的 Telnet 流量，这时就需要使用扩展访问控制列表，配置扩展访问控制列表也分为两个步骤：

1. 创建 ACL

在路由器 R2 上创建访问控制列表，配置如下：

```
R2 (config) #access-list 100 deny tcp host 12.1.1.1 host 23.1.1.3 eq Telnet
因为只拒绝 Telnet 流量，Telnet 流量使用的是 TCP 协议，目标端口是 23，所以这里拒绝的协议是 TCP，源地址是 R1，源端口任意（源端口没有指定，意指任意端口，其实源端口是大于 1023 以上的一个随机端口），目标地址是 R3，端口是 23（配置语句中的 Telnet 表示 23）。
R2 (config) #access-list 100 permit ip any any 隐含的是拒绝所有，这一行的作用是允许其他所有的 IP 流量通过。
```

上面两行的顺序同样很重要，不能颠倒。

2. 应用 ACL

创建好列表以后，接下来还必须将它应用到每个想用它的接口上。因为只想拒绝 R1 访问 R3 的 Telnet 流量，其他的访问不受影响，可以把列表用在 R2 的 S1/0 接口，当数据包进入 R2 的时候进行判断，配置如下：

```
R2 (config) #int s1/0
R2 (config-if) #ip access-group 100 in 在接口下调用访问控制列表 100，针对的是从 S1/0 接口进入路由器 R2 的流量。
```

两个步骤的操作顺序没有关系，但两个步骤缺一不可，创建列表没有在接口下调用，或者在接口下调用一个没有被创建的列表，都不会起作用。配置完成后，在 R1 上 ping 23.1.1.3，可以 ping 通；在 R1 上 Telnet 23.1.1.3，提示目标不可达，显示如下：

```
R1#ping 23.1.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.1.1.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/32/60 ms
R1#telnet 23.1.1.3
Trying 23.1.1.3 ...
% Destination unreachable; gateway or host down
```

在 R2 上 ping 23.1.1.3，可以 ping 通；在 R2 上 Telnet 23.1.1.3，可以连接，但提示虚拟终端密码没有设置，不允许远程登录，显示如下：

```
R2#ping 23.1.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.1.1.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/16/24 ms
R2#telnet 23.1.1.3
Trying 23.1.1.3 ... Open

Password required, but none set

[Connection to 23.1.1.3 closed by foreign host]
```

从上面显示可以看出，R1 和 R2 使用 Telnet 登录 R3，收到两种不同的提示，R1 看到的提示是目标不可达，而 R2 看到的提示是远程路由器 R3 没有配置远程登录密码。如果开通 R3 的远程登录和管理，需要在 R3 上进行如下配置：

```

R3(config)#line vty 0 4      配置虚拟终端接口。
R3(config-line)#login        要求登录。如输入 no login, 表示虚拟终端不需要登录, 可以直接进入。
                                出于安全考虑, 一般工程中都要求登录。
R3(config-line)#password cisco 虚拟终端的密码是 cisco。
R3(config-line)#exit
R3(config)#enable password cisco 特权密码是 cisco。

```

有些读者可能实验不成功, 该实验是在静态路由配置成功的基础上完成的, 请确信静态路由配置无误。如果读者是在标准访问控制列表的基础上, 继续配置扩展访问控制列表, 请删除标准访问控制列表。在 R3 上取消标准访问控制列表的配置如下:

```

R3(config)#no access-list 1
R3(config)#int s1/0
R3(config-if)#no ip access-group 1 in

```

扩展 ACL 的删除和取消在接口的调用与标准 ACL 相同, 这里不再介绍。

17.3.2 扩展 ACL 放置的位置***

列表写好以后, 可以用在哪台设备、哪个接口、哪个方向上, 还是有区别的。扩展 ACL 既可以控制源地址, 又可以控制目标地址。把 12.1.1.1 作为源地址, R3 就成为目标地址了, 数据流的方向就是从左到右, 如图 17-2-2 所示。从 R1 到 R3, 数据包共经过了 4 个接口, 如果用在 R1 的 S1/1 接口, 方向应该是 out; 如果用在 R2 的 S1/0 接口, 方向应该是 in; 如果用在 R2 的 S1/1 接口, 方向应该是 out; 如果用在 R3 的 S1/0 接口, 方向应该是 in。接下来分析把列表分别用在 4 个接口上有何不同, 可以通过实验来验证下面的结论。

- 如果把前面创建的扩展 ACL 100 配置在 R1 上, 并在 R1 的 S1/1 接口调用, 方向是 out。结果将不起作用, 原因是访问控制列表仅对穿越路由器的数据包进行过滤, 对本路由器起源的数据包不作过滤。
- 把前面创建的扩展 ACL 100 配置在 R2 上, 并在 R2 的 S1/0 接口调用, 方向是 in。结果正确, 并且无其他影响。
- 把前面创建的扩展 ACL 100 配置在 R2 上, 并在 R2 的 S1/1 接口调用, 方向是 out。结果正确, 并且无其他影响。
- 把前面创建的扩展 ACL 100 配置在 R3 上, 并在 R3 的 S1/0 接口调用, 方向是 in。结果正确, 并且无其他影响。

既然扩展 ACL 用在 R2 的两个接口和 R3 的一个接口上, 结果都正确, 并且都无其他影响, 那用在哪里更好一点呢? 如果扩展 ACL 应用在 R3 上, 一些非法的数据包到 R3 上被丢弃。如果扩展 ACL 应用在 R2 的 S1/0 接口上, 一些非法的数据包进入 R2 时将被丢弃。相比之下, 如果用在 R3 上, 不但占用了 R2 和 R3 之间的带宽, 而且浪费 R2 和 R3 更多的 CPU 资源, 用在 R2 上更合适。

从上面的分析中可以得出结论, 扩展 ACL 既可以控制源地址, 又可以控制目标地址, 不会带来负面影响, 尽量应用在靠近源端, 这样可以使一些非法的流量被尽早地丢弃, 节省中间设备的带宽和 CPU 资源。

17.3.3 扩展 ACL 的增强编辑功能*

本小节的内容相当有用, 但 CCNA 考试中不涉及本小节的内容, 读者可以选读这部分内容。

首先，对 Cisco 的 ACL 进行修改是件令人头疼的事情，因为 Cisco 的 ACL 只能向列表末尾添加语句，而不能在列表中间插入语句。有经验的工程师使用“show running-config”命令，查看正在运行的配置文件，从中拷贝出要修改的访问控制列表，在文本编辑器中修改 ACL，修改完成后，在路由器上删除正在使用的 ACL，再粘贴文本编辑中的 ACL。这样修改起来比直接在路由器上取消列表的所有行，再一条条输入要方便很多，但还是有点不方便，要取消列表，再应用。Cisco 在 IOS 12.2T8 及以后的版本中增强了扩展 ACL 的修改功能，用户可以向现存 ACL 的任意位置插入新的语句。如何判断正在使用的 IOS 是否支持扩展访问控制列表的增强编辑功能，记住 IOS 的版本太困难了，这里告诉大家一个直观的方法，比如在路由器 R2 上执行“show access-list 100”命令，有下面的输出：

```
R2#show access-lists
Extended IP access list 100
 10 deny tcp host 12.1.1.1 host 23.1.1.3 eq Telnet (5 matches)
 20 permit ip any any
```

这里的 10 是行号，5 matches 表示这条 ACL 指令被匹配到 5 次，有时不容易看到结果的实验，可以借助访问控制列表中的匹配数来辅助测试。

从输出中如果可以看到列表中每条语句之前加了行号（10 和 20），那么正在使用的 IOS 就支持扩展 ACL 的增强编辑功能。下面演示如何在路由器 R2 上向列表中间插入新的语句，以及验证插入语句后的 ACL。操作和输出如下：

```
R2(config)#ip access-list extended 100
R2(config-ext-nacl)#15 permit ip host 1.1.1.1 host 2.2.2.2
R2(config-ext-nacl)#do show access-list 100
Extended IP access list 100
 10 deny tcp host 12.1.1.1 host 23.1.1.3 eq Telnet (5 matches)
 15 permit ip host 1.1.1.1 host 2.2.2.2
 20 permit ip any any
```

在中间成功插入了一个新行。

从上面的输出中可以看到，由于新插入语句的行号为 15，因此它插在了行号为 10 和 20 的两句话中间。可以使用“ip access-list resequence access-list-number start-number increase-number”命令对访问控制列表的序列号进行重新编号，其中“access-list-number”是列表号，“start-number”是列表的起始行号，“increase-number”是每一行的增量。例如：

```
R2(config)#ip access-list resequence 100 30 20
R2(config)#do show access-list 100
Extended IP access list 100
 30 deny tcp host 12.1.1.1 host 23.1.1.3 eq Telnet (3 matches)
 50 permit ip host 1.1.1.1 host 2.2.2.2
 70 permit ip any any
```

在“ip access-list resequence 100 30 20”命令中，100 表示扩展访问控制列表的编号，30 表示起始的行号，20 表示增量，每一行递增 20，得到新编号的行号是 30、50、70。标准 ACL 不支持这种中间插入的方式。

这种扩展 ACL 的增强编辑功能也允许动态地删除一条指令，使用方法如下：

```
R2(config)#ip access-list extended 100
R2(config-ext-nacl)#no 30
```

只需要删除行号，则该行的对应内容被自动删除。

17.3.4 扩展 ACL 中的 established**

配置使用 TCP 协议的扩展 ACL 时，有一个参数 established（已建立），特别值得关注，它可以用来做 TCP 的单向访问控制，使用起来有点像防火墙，一边可以访问另外一边，另外一边却不能访问这一边。established 主要是利用 TCP 协议的特点，在 TCP 会话中，是通

过初始的数据包中只有 Sequence（序列号），而没有 ACK（确认号）来实现的。针对被保护的网路，只允许 established 的 TCP 包进入，如果是从外部主动发起到受保护网络的连接，因为连接尚未建立，这样 TCP 包不允许进入。如果是受保护网络主动发起到外部的连接，外部返回的数据包将携带 ACK 参数，这样的 TCP 被认为是已建立的，允许进入受保护网络。比如在图 17-2-1 中，实现 R1 不可以 Telnet R3，但 R3 可以 Telnet R1。

结合图 17-2-1，可以把 R3 想象成内网，R2 想象成边界路由器，R1 想象成外网。当外界有 TCP 流量欲通过 R2 的 S1/1 接口访问内网时，R2 上的访问控制列表，判断该数据包中有没有设置 ACK 位（也就是连接是否已建立，established），如果有，说明这个包不是第一个发起的包，允许通过；如果没有设置 ACK 位（也就是连接的发起者，连接尚未建立），不满足 established 条件，丢弃数据包。该实验的步骤如下：

步骤 1：基本配置。如 17.2.2 节所示，配置 R1、R2、R3，保证网络连通性。读者也可以在前一个实验的基础上，取消 R2 上的无关配置来实现。

步骤 2：配置远程登录。配置 R1 和 R3 的 VTY 密码和特权密码，以允许远程登录，并在 R1 上 Telnet R3，在 R3 上 Telnet R1 进行测试。

配置 R1，允许远程登录，命令如下：

```
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#enable password cisco
```

配置 R3，允许远程登录，命令如下：

```
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#enable password cisco
```

配置完成后，测试远程登录情况，R1 和 R3 均可正常登录到对方。

步骤 3：配置访问控制列表。在 R2 上进行如下配置：

```
R2(config)#access-list 100 permit tcp any any established
R2(config)#int s1/1
R2(config-if)#ip access-group 100 out
```

步骤 4：测试。

在 R1 上登录 R3，显示如下：

```
R1#telnet 23.1.1.3
Trying 23.1.1.3 ...
% Destination unreachable; gateway or host down
```

R1 远程登录 R3 失败。接下来在 R3 上登录 R1，显示如下：

```
R3#telnet 12.1.1.1
Trying 12.1.1.1 ... Open
User Access Verification
Password:
R1>en
Password:
R1#
```

R3 远程登录 R1 成功。访问控制列表 100 作为出站列表应用在 R2 的 S1/1 接口上，也就是说，从 12.1.1.1 发往 23.1.1.3 的 TCP 数据包必须是已建立的，否则会被拒绝。

如果在 R3 上 ping R1 的 IP 地址会怎样呢？测试如下：

```
R3#ping 12.1.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

不管是 R1 ping R3, 还是 R3 ping R1 都是失败。原因是因为 R2 的 S1/1 接口仅允许 TCP 中 established 的流量通过, 并不允许 ICMP 协议。如果想 R3 可以 ping 通 R1, R1 不可以 ping 通 R3, 在访问控制列表中添加下面的一行指令:

```
R2(config)#access-list 100 permit icmp any any echo-reply
```

R1 主动 ping R3 的数据包, 发出的是 ICMP 的 echo 报文, 不允许通过。而 R3 ping R1, 从 R1 返回的报文是 ICMP 的 echo-reply 报文, 允许通过。

测试: 在 R3 上 ping R1 成功, 在 R1 上 ping R3 失败。

! 注意: established 只能用于基于 TCP 的应用, 例如 Telnet、FTP、HTTP 等。对基于 UDP、ICMP 等协议则不起作用。后面将要介绍的自反访问控制列表可以很好地解决这一缺陷。

17.3.5 配置扩展命名 ACL**

扩展命名 ACL 的用法与标准命名 ACL 的用法类似, 这里仅举一个简单的应用。本章 17.3.4 小节 R2 上的编号扩展列表用命名扩展 ACL 表示, 实现如下:

```
R2(config)#ip access-list extended tcp-firewall
R2(config-ext-nacl)#permit tcp any any established
R2(config-ext-nacl)#permit icmp any any echo-reply
R2(config-ext-nacl)#int s1/1
R2(config-if)#ip access-group tcp-firewall out
```



17.4 配置 ACL 的注意事项***

前面 3 节介绍了标准、扩展和命名访问控制列表。本节介绍应用访问控制列表的一些注意事项:

- (1) 访问控制列表只对穿越流量起作用。本章 17.2.4 节有叙述。
- (2) 标准列表要应用在靠近目标端。本章 17.2.4 节有叙述。
- (3) 扩展访问控制列表要应用在靠近源端。本章 17.3.2 节有叙述。
- (4) 放置的顺序。配置 ACL 时, 语句的前后顺序很重要, 列表从上往下查找, 如果找到一条匹配, 就执行操作并且不再往下继续查找。如果两条语句放在前或后都不影响结果, 一般把被较多使用的那条放在前面, 这样可以减小路由器的查找时间。
- (5) 隐含的拒绝所有。IP 访问控制列表的最后一句隐含的是拒绝所有。它表示必须明确允许通信量, 否则将被拒绝。
- (6) 列表的编辑。访问控制列表建立后, 对该 ACL 的增加都被放在表的末端, 用户不能有选择地增加或删除语句。唯一可做的删除是删除整个访问控制列表, 命令是 “no access-list access-list-number”, 显然, 当访问控制列表很大时是十分麻烦的。为了节省时间, 可以将表剪切, 然后粘贴在文本文档中来编辑。命名访问控制列表和扩展访问控制列表的增强编辑功能可用于克服这一缺点。
- (7) 列表的调用。一个访问控制列表可用于同一个路由器的许多不同的接口上, 并不需要对每个需要它的接口单独定义表号不同、内容相同的访问控制列表。如果不给接口提供任何访问控制列表, 或者提供一个未定义的访问控制列表, 则在默认情况下它将传递所

(8) 使用 ACL 限制远程登录。值得一提的是, 如果想限制登录某台设备, 应该进入虚拟终端线路, 使用 `access-class` 来实现, 而不是在所有接口上限制 Telnet 登录。配置如下:

上面对路由器 R2 的配置，将实现只有 12.1.1.1 可以远程登录 R2，其他的 IP 地址将不被允许。非法的远程登录，将收到下面的提示信息：

(9) 配置 ACL 时, 小心不要拒绝了路由协议。下面举例说明这个问题, 配置 RIP 协议, 实现如图 17-4-1 所示的网络互连。配置 ACL, 允许 R1 到 R3 的所有 IP 地址访问。除了远程登录外, 禁止 R2 到 R3 的所有 IP 服务。



```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
R1(config-if)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#enable pass cisco
R1(config)#router rip
R1(config-router)#net 12.0.0.0
```

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#router rip
R2(config-router)#net 12.0.0.0
R2(config-router)#net 23.0.0.0
```

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#line vty 0 4
R3(config-line)#password cisco
```

```
R3(config-line)#login
R3(config-line)#enab pass cisco
R3(config)#router rip
R3(config-router)#net 23.0.0.0
```

RIP 配置完成后, R1、R2、R3 之间的访问完全正常。接下来配置 ACL, 因为要限制 R2 对 R3 的访问, ACL 配置在 R2 S1/1 接口的外出方向将不起作用, 因为 ACL 对本路由器起源的流量不起作用。这里把 ACL 配置在 R3 上, 因为涉及流量的类型, 这里使用扩展 ACL。R3 的配置如下:

```
R3(config)#access-list 100 permit ip host 12.1.1.1 host 23.1.1.3
允许R1到R3的所有IP流量, IP整套协议都将被允许。
R3(config)#access-list 100 permit tcp host 23.1.1.2 host 23.1.1.3 eq 23
只允许R2远程登录R3, 其他流量均被默认拒绝。
R3(config)#int s1/0
R3(config-if)#ip access-group 100 in
```

配置完成后, 在 R1 上 ping 和 Telnet R3, 结果均正常。在 R2 上 Telnet R3 正常, ping R3 失败。这样似乎完成了需求, 果真如此吗?

在 R3 上使用 “debug ip routing” 命令监测路由表的变化, 大约 240 秒左右, R3 的控制台显示如下:

```
R3#debug ip routing
IP routing debugging is on
R3#
*Mar 1 00:26:13.531: RT: delete route to 12.0.0.0 via 23.1.1.2, rip metric [120/1]
*Mar 1 00:26:13.535: RT: SET_LAST_RDB for 12.0.0.0/8
OLD rdb: via 11.13.11.13
*Mar 1 00:26:13.539: RT: no routes to 12.0.0.0, entering holddown
*Mar 1 00:26:13.539: RT: NET-RED 12.0.0.0/8
```

上面的信息显示 R3 上去往 12.0.0.0 的路由消失了, 查询 R3 的路由表, 显示如下:

```
R3#show ip route
23.0.0.0/24 is subnetted, 1 subnets
C 23.1.1.0 is directly connected, Serial1/0
```

从 R3 的路由表可以得知, 从 R2 学来的关于 12.0.0.0 的 RIP 路由条目消失了, R1 此时与 R3 的任何通信都是失败的。为什么刚开始都是正常的, 一段时间后会网络故障呢? 类似于这样, 不会马上出现故障的问题是比较隐蔽的, 排查起来相对也困难。

因为这里运行的是动态路由协议, R2 要周期性地把自己的路由表发给 R3, 可是 R3 的 S1/0 接口在入站方向应用了 ACL 100, 阻止了 R2 的 RIP 更新包。之所以没有马上出现故障现象, 是因为 RIP 协议删除路由条目的时间是 240 秒。

这里除了允许 R2 去往 R3 的 Telnet 流量外, 还应该允许 R2 去往 R3 的 RIP 更新流量。分析 RIP 协议的特点, RIP 更新使用的是 UDP 协议的 520 端口, 修改 R3 上的 ACL 100, 允许 R2 的 UDP 更新包进入。命令如下:

```
R3(config)#access-list 100 permit udp host 23.1.1.2 host 255.255.255.255 eq 520
因为RIPv1是广播式更新, 目标IP地址是255.255.255.255, 目标端口是520。这里读者也可以粗略地写成access-list 100 permit udp any any eq 520。
```

稍后 R3 重新学到了 12.0.0.0 的路由。通过这个简单的实验, 可以看出, 在实际工程中配置 ACL 要非常小心, 考虑全面。



17.5 复杂 ACL

本节介绍几个复杂的 ACL: 反射 ACL、动态 ACL 和基于时间的 ACL。

17.5.1 反射 ACL

17.3.4 节介绍的单向访问控制方法是使用 ACL 中的 `established` 参数检测 TCP 段中是否有 ACK 位来实现的，但这种方法仅用于基于 TCP 的上层协议，而对于其他上层协议（如 UDP、ICMP 等）则无法实现单向访问控制。

这里介绍的 **Reflexive ACL**（反射 ACL，很多文档中也称自反 ACL）提供了一种真正意义上的单向访问控制，它的工作原理是：当内部网络发起一个会话（基于 IP、ICMP、TCP、UDP 的都可以），并且将数据发送给外部网络时，反射 ACL 被触发并且生成一个新的临时条目。如果从外部网络回来的数据流符合临时条目，则允许其进入内部网络，否则禁止其进入内部网络，如图 17-5-1 所示。反射 ACL 真正起到了防火墙的作用，反射 ACL 不仅检查数据包中的 ACK 和 RST 比特位，还检查源和目标地址及端口号，可以很好地阻止欺骗和某些类型的 DoS（Denial of Service，拒绝服务）攻击。

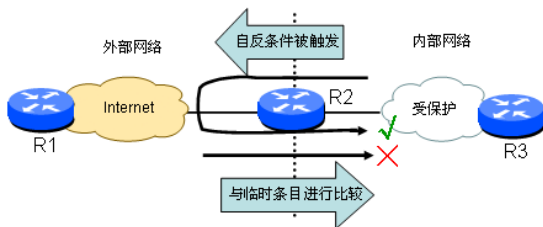


图 17-5-1 反射 ACL

注意： Cisco IOS 只支持使用扩展的命名访问控制列表来定义反射列表。

下面结合图 17-2-1 来讲解反射访问控制列表的配置。

在图 17-2-1 中，路由器 R1 相当于外网的一台主机，路由器 R3 相当于内网的一台主机，路由器 R2 相当于企业的边界路由器。使用反射列表配置路由器 R2，使 R3 可以 ping 通 R1，但 R1 却 ping 不通 R3；使 R3 可以 Telnet 登录 R1，但 R1 却不能 Telnet 登录 R3。由内网（R3）始发的流量到达配置了反射 ACL 的路由器（R2），路由器根据此流量的第三层和第四层信息自动生成一个临时性的访问表。临时性访问表的创建依据下列原则：**protocol** 不变，**Source-IP** 地址和 **Destination-IP** 地址严格对调，**Source-port** 和 **Destination-port** 严格对调，对于 ICMP 这样的协议，会根据类型号进行匹配。路由器将此流量传出，流量到达目标（R1），然后响应流量从目标返回到配置了反射 ACL 的路由器 R2。路由器 R2 对入站的相应流量进行评估，只有当返回流量的第三层、第四层信息与先前基于出站流量创建的临时性访问表的第三层、第四层信息严格匹配时，路由器才会允许此流量进入内部网络。该实验的配置步骤如下：

步骤 1：基本配置。如 17.2.2 节所示，配置 R1、R2、R3，保证网络连通性。读者也可以在前一个实验的基础上，取消 R1、R2 和 R3 上的无关配置来实现。

步骤 2：配置远程登录。配置 R1 和 R3 的 VTY 密码和特权密码，以允许远程登录，并在 R1 上 Telnet R3，在 R3 上 Telnet R1 进行测试。

步骤 3：配置反射列表。R2 上的反射 ACL 配置如下，其中斜体部分为注释：

```
R2(config)#ip access-list extended out-acl    创建扩展的命名 ACL，名字叫 out-acl，用在路
                                              由器 R2 外部接口 S1/0 的外出方向。
R2(config-ext-nacl)#permit ip any any reflect out-ip
                                              允许所有的 IP 流量，并对外出的 IP 流量进行反射，反射的名字叫 out-ip，其实就是创建临时的访问控制列表。
R2(config-ext-nacl)#exit
R2(config)#ip access-list extended in-acl    创建扩展的命名 ACL，名字叫 in-acl，用在路由
                                              器 R2 外部接口 S1/0 的进入方向。
```

```
R2(config-ext-nacl)#evaluate out-ip    评估反射列表，其实就是调用前面创建的临时列表。
R2(config-ext-nacl)#int S 1/0
R2(config-if)#ip access-group out-acl out    调用访问控制列表，要注意方向，外出的时候做反射。
R2(config-if)#ip access-group in-acl in    调用访问控制列表，要注意方向，进入的时候做评估。
```

步骤 4：再次测试 ping 和 Telnet。

在 R3 上 Telnet 和 ping R1，显示如下，都是成功的：

```
R3#ping 12.1.1.1
*Mar  1 00:06:07.387: %SYS-5-CONFIG I: Configured from console by console
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/44/72 ms
R3#telnet 12.1.1.1
Trying 12.1.1.1 ... Open
User Access Verification
Password:
R1>en
Password:
R1#
```

先不要在 R3 上退出 R1 的远程登录界面。

在 R1 上 Telnet 和 ping R3，显示如下，都是失败的：

```
R1#telnet 23.1.1.3
Trying 23.1.1.3 ...
% Destination unreachable; gateway or host down
R1#ping 23.1.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.1.1.3, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R1#
```

在路由器 R2 上查看访问控制列表，可以发现反射访问列表 out-ip 下多出两个临时条目，超时时间默认是 300 秒。

```
R2#show access-lists
Extended IP access list in-acl
  10 evaluate out-ip
Extended IP access list out-acl
  10 permit ip any any reflect out-ip (308 matches)
Reflexive IP access list out-ip
  permit tcp host 12.1.1.1 eq telnet host 23.1.1.3 eq 45503 (117 matches) (time left 277)
  permit icmp host 12.1.1.1 host 23.1.1.3 (19 matches) (time left 270)
```

“time left 277”和“time left 270”表示该条目被删除前还剩下的时间。反射列表生成的临时条目在会话结束后应当被删除。对于 TCP 会话，如果路由器检测到两组 FIN 标记的分组，则在 5 秒内将临时条目删除；如果路由器检测到 RST 位的分组（说明会话突然关闭），则立刻删除临时条目。对于 UDP 和其他协议，由于没有专门的机制来判断会话是否结束，因此路由器只能为其会话启动一个倒计时的计时器（全局超时），如果在计时器到期时没有收到此会话的任何分组，则将临时条目删除（默认 300 秒）。

可以使用“ip reflexive-list timeout seconds”命令对全局超时时间进行修改。下面的命令把超时时间从 300 秒改成 60 秒。

```
R2(config)#ip reflexive-list timeout 60
```

在 R3 上退出 R1 的远程登录，马上在 R2 上查看访问控制列表，显示如下：

```
R2#show access-lists
Extended IP access list in-acl
```

```

10 evaluate out-ip
Extended IP access list out-acl
10 permit ip any any reflect out-ip (308 matches)
Reflexive IP access list out-ip
  permit tcp host 12.1.1.1 eq telnet host 23.1.1.3 eq 27225 (117 matches) (time left 2)
  permit icmp host 12.1.1.1 host 23.1.1.3 (19 matches) (time left 147)

```

从上面的输出中，注意到当断开 TCP 会话时，剩下的时间迅速减小到 2 秒。稍后再次查看 R2 上的访问控制列表，显示如下：

```

R2#show access-lists
Extended IP access list in-acl
10 evaluate out-ip
Extended IP access list out-acl
10 permit ip any any reflect out-ip (308 matches)
Reflexive IP access list out-ip
  permit icmp host 12.1.1.1 host 23.1.1.3 (19 matches) (time left 30)

```

从上面的输出中注意到，“permit tcp host 12.1.1.1 eq telnet host 23.1.1.3 eq 27225”条目已经被删除。“permit icmp host 12.1.1.1 host 23.1.1.3”条目过 30 秒也将被删除。

17.5.2 动态 ACL

这里介绍动态 ACL，动态 ACL 是对传统 ACL 的一种功能增强。传统的标准 ACL 和扩展 ACL 不能创建动态访问条目。一旦在传统 ACL 中加入了一个语句，除非手工删除，否则该语句将一直产生作用。而在动态 ACL 中，网络管理员可以根据用户验证过程来创建特定的、临时的 ACL。

动态 ACL 使用扩展 ACL 过滤 IP 流量，当配置了动态 ACL 之后，临时被拒绝掉的 IP 流量可以获得暂时性的许可。动态 ACL 临时修改路由器接口下已经存在的 ACL，来允许 IP 流量到达目标设备，之后动态 ACL 把接口状态还原。通过动态 ACL 获得访问目标设备权限的用户，首先要开启到路由器的 Telnet 会话，接着动态 ACL 自动对用户进行验证，如果验证通过，那么用户就获得了临时性的访问权限。

动态 ACL 一般用于控制外网用户对内网服务器的访问，如图 17-5-2 所示，当 Internet 上的用户需要访问内网的服务器时，外网用户需要先向路由器发起一个 Telnet 会话，并且提供相应的用户名和密码。在用户被验证之后，路由器将一个临时的 ACL 语句添加到动态 ACL 中，并且关闭 Telnet 会话。动态添加的 ACL 对被验证用户工作站地址进行授权，当条目超时后，删除动态 ACL 中添加的临时条目。

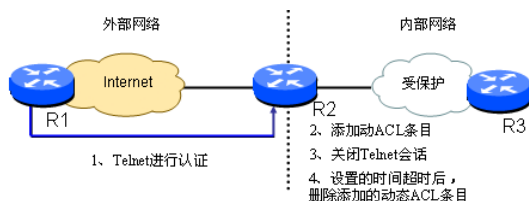


图 17-5-2 动态 ACL 原理图

通过使用动态 ACL 不仅为授权用户提供了一个访问受保护网络的通道，还可以有效阻止未授权用户的访问和黑客的攻击。

(1) 临时条目的生存周期

和反射 ACL 一样，动态 ACL 也会创建临时条目，其生存周期有两个参数：空闲时间和绝对时间。当路由器产生临时条目时，该临时条目的空闲计时器和绝对计时器同时启动。空闲计时器在每当有一个报文匹配动态访问表项时进行复位，当空闲计时器到期时，该临时条目被删除。绝对计时器永不复位，当绝对计时器到期时，该临时条目被删除，而忽略空闲计时器的值和当前连接状态。在通常情况下，绝对时间应设置得大一些，比如 24 小时；

而空闲时间应设置得远远小于绝对时间，比如 5 分钟。

(2) Telnet 的设置

设置了动态 ACL 以后，所有的 Telnet 请求都会被路由器认为是要开启一个动态 ACL 条目，当用户被验证之后，Telnet 会话很快就会被关闭。这就带来了一个问题，网络管理员将不再能够通过 Telnet 对路由器进行管理。

解决上述问题的方法是，在一部分 VTY 线路上使用 rotary(旋转)命令开启其他的 Telnet 端口，例如：“rotary 1”命令开启 3001 端口，“rotary 2”命令开启 3002 端口，依此类推。

(3) 配置动态 ACL

在图 17-5-2 中，希望使用动态 ACL 实现：让 Internet 上的用户(R1)需要访问内网(R3)时，先到路由器 R2 上验证，验证通过后则可以访问内网。该实验的配置步骤如下：

步骤 1：基本配置。如 17.5.1 节所示，配置 R1、R2、R3，保证网络连通性，并配置 R1 和 R3 的远程登录功能。

步骤 2：测试。R1 和 R3 相互 Telnet 或 ping 对方的 IP 地址，都是成功的。

步骤 3：动态 ACL 配置。路由器 R2 上动态 ACL 的配置如下：

```
R2(config)#access-list 100 permit tcp any host 12.1.1.2 eq 23 允许外网 Telnet 路由
器进行身份验证。
R2(config)#access-list 100 permit tcp any host 12.1.1.2 eq 3001
允许外网 Telnet 路由器的 3001 端口进行管理，工程中，很少在 Internet 上使用 Telnet，因为密码明文
传输，很不安全。如果工程中使用的是其他网管协议，记得开放对应的端口。
R2(config)#access-list 100 dynamic cisco timeout 120 permit ip any any
创建动态 ACL，命名为 cisco，该语句中的第一个 any 关键字将被通过验证的用户的 IP 地址替代，第二个 any
代指内网所有主机。当然这里可以变成特定的主机，这样做的结果是：即使外网用户通过路由器的验证也只能
访问内网中的特定主机；还可以把 IP 协议换成其他协议，比如 TCP 的 80，这样做的结果是：即使外网用户通
过路由器的验证也只能访问内网中特定主机 TCP 的 80 端口，也就是 Web 主页。timeout 是绝对时间，120
分钟，也就是两个小时。
R2(config)#user cisco pass cisco 创建用户 cisco，用于身份验证。
R2(config)#line vty 0 3 虚拟终端用户 0, 1, 2, 3。
R2(config-line)#login local 使用路由器本地的用户名和密码验证。
R2(config-line)#autocommand access-enable host timeout 5
这里的参数输入一定要正确，即使输入错误也没有提示，其中 host 参数的意思是验证主机的源 IP 地址替换动
态 ACL 中的 any 关键字，timeout 时间是指空闲时间，其后面的 5 代表 5 分钟。
R2(config-line)#line vty 4 虚拟终端用户 4。
R2(config-line)#login local 使用路由器本地的用户名和密码验证。
R2(config-line)#rotary 1 设置 VTY 4 号线路为管理员使用 Telnet 对路由器进行
管理，Telnet 端口为 3001。
R2(config-line)#int S 1/0
R2(config-if)#ip access-group 100 in 在路由器外网接口上应用 ACL。
```

步骤 4：测试。在 R3 上 Telnet R1，是失败的，显示如下：

```
R3#telnet 12.1.1.1
Trying 12.1.1.1.
% Destination unreachable; gateway or host down
```

这是因为 R3 去往 R1 的流量没有问题，当 R1 返回 R3 的流量进入路由器 R2 的 S1/0 接口时，该接口配置了一个入站的访问控制列表 100，该列表拒绝 R1 返回 R3 的流量，Telnet 失败。同理，R3 ping R1 也失败。

在 R1 上 Telnet R3，也是失败的，显示如下：

```
R1#telnet 23.1.1.3
Trying 23.1.1.3 ...
% Destination unreachable; gateway or host down
```

这是因为 R1 去往 R3 的 Telnet 数据包进入路由器 R2 的 S1/0 接口时，被路由器 R2 的

ACL 100 拒绝。同理，R1 ping R3 也是失败的。

在 R1 上 Telnet 路由器 R2 的外网接口 12.1.1.2, 要求验证, 输入用户名 cisco、密码 cisco, 验证通过, Telnet 会话自动被终止。在 R1 上再次 Telnet R3, 成功远程登录, 在 R1 上 ping R3, 也可以 ping 通, 显示如下:

```
R1#telnet 23.1.1.3
Trying 23.1.1.3 ...
% Destination unreachable; gateway or host down
```

R1 登录 R3 失败。

```
R1#telnet 12.1.1.2
Trying 12.1.1.2 ... Open
User Access Verification
Username: cisco
Password:
[Connection to 12.1.1.2 closed by foreign host]
```

R1 成功地登录了 R2, 登录成功后, R2 会自动断开连接。

```
R1#telnet 23.1.1.3
Trying 23.1.1.3 ... Open
User Access Verification
Password:
R3>en
Password:
R3#
```

在 R2 上验证成功后, 此时 R1 可以成功地远程登录到 R3。

```
R3#exit
[Connection to 23.1.1.3 closed by foreign host]
```

断开远程登录, 返回到 R1。

```
R1#ping 23.1.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.1.1.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/21/24 ms
```

R1 可以成功地 ping 通 R3。同样测试 R3 到 R1 的 ping 或 Telnet, 结果也是成功的。在路由器 R2 上使用 “show access-lists” 命令查看 ACL, 显示如下:

```
R2#show access-lists
Extended IP access list 100
 10 permit tcp any host 12.1.1.2 eq telnet (72 matches)
 20 permit tcp any host 12.1.1.2 eq 3001
 30 Dynamic cisco permit ip any any
    permit ip host 12.1.1.1 any (45 matches) (time left 295)
```

从上面的输出中可以看到, 最后一行是动态 ACL 产生的一个条目, 该条目再过 295 秒将被删除。有任何符合 “permit ip host 12.1.1.1 any” 的流量, 都会刷新该计时器, 如果没有任何流量来刷新计时器, 这个动态条目将在 295 秒后被删除。

动态 ACL 配置成功后, R1 将不能使用常用的 Telnet 对 R2 进行远程管理, 因为常用的 23 号 Telnet 端口, 已经被用来做动态 ACL 授权了。这里需要使用 3001 端口, 对 R2 进行远程管理, 显示如下:

```
R1#telnet 12.1.1.2 3001
Trying 12.1.1.2, 3001 ... Open
User Access Verification
Username: cisco
Password:
R2>
```


17.5.3 基于时间的 ACL

基于时间的 ACL 是对传统 ACL 的一种功能增强，它在传统的扩展 ACL 中加入了时间范围以增强 ACL 的控制功能。要使用基于时间的 ACL，首先要创建一个时间范围，然后在扩展 ACL 中进行调用。创建时间范围的命令格式如下：

```
R1(config)#time-range working 定义时间范围的名字，这里使用的名字是 working
R1(config-time-range)#? 寻求在线帮助。
Time range configuration commands:
    absolute absolute time and date 定义绝对时间范围，从某年某月某日某时某分开始，或至某年
    某月某日某时某分结束，这里的月份要用英文表示。
    default Set a command to its defaults
    exit Exit from time-range configuration mode
    no Negate a command or set its defaults
    periodic periodic time and date
    定义周期性的时间范围，可以是星期几（记得要写英文）、daily（每天）、weekday（周一至周五）、weekend
    （周末）和时间（hh:mm）参数。
```

! 注意：Cisco IOS 只支持使用扩展访问控制列表定义基于时间的 ACL。

下面举一个例子来说明基于时间的 ACL 的定义方法。假如某单位希望在企业出口路由器上使用基于时间的 ACL 实现：周一到周五（工作日）的上午从 8:00 到 12:00，下午从 13:30 到 17:30 只允许用户收发邮件，非工作时间允许所有的访问。实验的配置步骤如下：

步骤 1：配置路由器的时间。基于时间的 ACL 能正常工作的前提是在路由器的特权模式下，使用 `clock set` 调整路由器的时间。

步骤 2：定义时间范围。

```
Router(config)#time-range working 定义上班时间范围。
Router(config-time-range)#periodic weekdays 8:00 to 12:00 周一至周五每天从 8 点到 12 点。
Router(config-time-range)#periodic weekdays 13:30 to 17:30
周一至周五每天从 13:30 到 17:30，两个时间加起来就是从早 8 点到下午的 5 点半，除去中午一个半小时的
休息时间。
```

步骤 3：编辑 ACL。

```
Router(config)#access-list 100 permit tcp any any eq 25 允许发送邮件。
Router(config)#access-list 100 permit tcp any any eq 110 允许接收邮件。
Router(config)#access-list 100 permit udp any any eq 53 允许使用外网的 DNS 服务器。
Router(config)#access-list 100 deny ip any any time-range working 在工作时间阻止所有的 IP 通信。

Router(config)#access-list 100 permit ip any any 允许所有的 IP 通信。
```

步骤 4：调用 ACL。

```
Router(config)#int fa 0/0 进入对外接口。
Router(config-if)#ip access-group 100 out 调用访问控制列表。
```

打开 Dynamips 机架中的 R1 和 R2，配置基于时间的 ACL，实现只有在周一到周五（工作日）的上午从 8:00 到 12:00，下午从 13:30 到 17:30，R1 才可以 Telnet R2。

R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
```

R2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#line vty 0 4
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#clock timezone gm +8          配置时区, 中国在东八区。
R2(config)#exit
R2#clock set 10:30:00 1 jan 2010         配置时间为 2010 年 1 月 1 号 10: 30 分。
R2#conf t
R2(config)#time-range working           定义一个时间范围。
R2(config-time-range)#periodic weekdays 8:00 to 12:00
R2(config-time-range)#periodic weekdays 13:30 to 17:30
R2(config-time-range)#exit
R2(config)#access-list 100 permit tcp host 12.1.1.1 host 12.1.1.2 time-range working
eq 23 创建基于时间的 ACL。
R2(config)#int s1/0
R2(config-if)#ip access-group 100 in
```

在 R1 上尝试登录 R2, 登录成功。更改 R2 的时间到晚上 18:00 点, 然后在 R1 上再次尝试登录 R2, 登录失败。

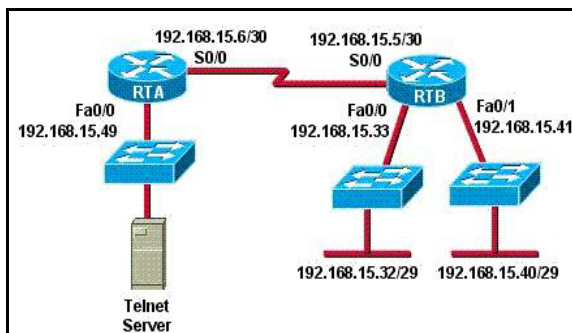


17.6 真题精选***

1. What three pieces of information can be used in an extended access list to filter traffic? (Choose three.)

- A. protocol
- B. VLAN number
- C. TCP or UDP port numbers
- D. source switch port number
- E. source IP address and destination IP address
- F. source MAC address and destination MAC address

2. Refer to the exhibit. The access list has been configured on the S0/0 interface of router RTB in the outbound direction. Which two packets, if routed to the interface, will be denied? (Choose two.)



```
access-list 101 deny tcp 192.168.15.32 0.0.0.15 any eq telnet
```

```
access-list 101 permit ip any any
```

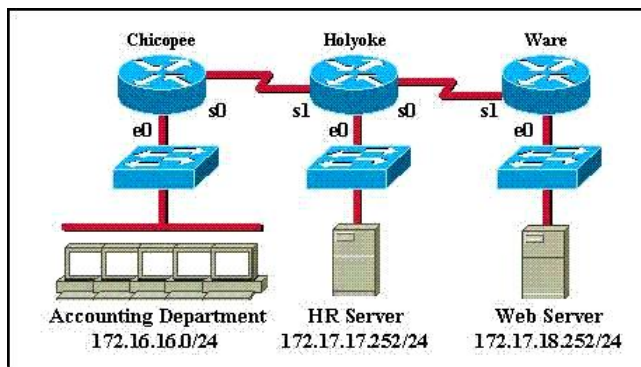
- A. source ip address: 192.168.15.5; destination port: 21
- B. source ip address:, 192.168.15.37 destination port: 21
- C. source ip address:, 192.168.15.41 destination port: 21
- D. source ip address:, 192.168.15.36 destination port: 23
- E. source ip address: 192.168.15.46; destination port: 23
- F. source ip address:, 192.168.15.49 destination port: 23

3. What is the effect of the following access list condition?

```
access-list 101 permit ip 10.25.30.0 0.0.0.255 any
```

- A. permit all packets matching the first three octets of the source address to all destinations
- B. permit all packets matching the last octet of the destination address and accept all source addresses
- C. permit all packets from the third subnet of the network address to all destinations
- D. permit all packets matching the host bits in the source address to all destinations
- E. permit all packets to destinations matching the first three octets in the destination address

4. An access list has been designed to prevent HTTP traffic from the Accounting Department from reaching the HR server attached to the Holyoke router. Which of the following access lists will accomplish this task when grouped with the e0 interface on the Chicopee router?



- A. permit ip any any
deny tcp 172.16.16.0 0.0.0.255 172.17.17.252 0.0.0.0 eq 80
- B. permit ip any any
deny tcp 172.17.17.252 0.0.0.0 172.16.16.0 0.0.0.255 eq 80
- C. deny tcp 172.17.17.252 0.0.0.0 172.16.16.0 0.0.0.255 eq 80
permit ip any any
- D. deny tcp 172.16.16.0 0.0.0.255 172.17.17.252 0.0.0.0 eq 80
permit ip any any

5. Drop :

Drag and drop question. Drag the items to the proper locations.

The Missouri branch office router is connected through its s0 interface to the Alabama Headquarters router s1 interface. The Alabama router has two LANs. Missouri users obtain Internet access through the Headquarters router. The network interfaces in the topology are addressed as follows: **Missouri:** e0 - 192.168.35.17/28; s0 - 192.168.35.33/28; **Alabama:** e0 - 192.168.35.49/28; e1 - 192.168.35.65/28; s1 - 192.168.35.34/28. The accounting server has the address of 192.168.35.66/28. Match the access list conditions on the left with the goals on the right. (Not all options on the left are used.)

deny ip 192.168.35.55 0.0.0.0 host 192.168.35.66	Block only the users attached to the e0 interface of the Missouri router from access to the accounting server.
deny ip 192.168.35.16 0.0.0.15 host 192.168.35.66	Block a user from the Alabama e0 network from access to the accounting server.
permit ip any any	Prevent all users from outside the enterprise network from accessing the accounting server.
permit ip 192.168.35.0 0.0.0.255 host 192.168.35.66	

6. A host with the address of 192.168.125.34 /27 needs to be denied access to all hosts outside its own subnet. To accomplish this, complete the command in brackets, [access-list 100 deny protocol address mask any], by dragging the appropriate options on the left to their correct placeholders on the right.

A host with the address of 192.168.125.34 /27 needs to be denied access to all hosts outside its own subnet. To accomplish this, complete the command in brackets, [access-list 100 deny protocol address mask any], by dragging the appropriate options on the left to their correct placeholders on the right.

0.0.0.0	protocol
192.168.125.0	
192.168.125.32	address
192.168.125.34	
255.255.255.255	mask
ip	
tcp	
udp	

Drag and drop question. Drag the items to the proper locations.

7. An access list was written with the four statements shown in the graphic. Which single access list statement will combine all four of these statements into a single statement that will have exactly the same effect?

```
access-list 10 permit 172.29.16.0 0.0.0.255
access-list 10 permit 172.29.17.0 0.0.0.255
access-list 10 permit 172.29.18.0 0.0.0.255
access-list 10 permit 172.29.19.0 0.0.0.255
```

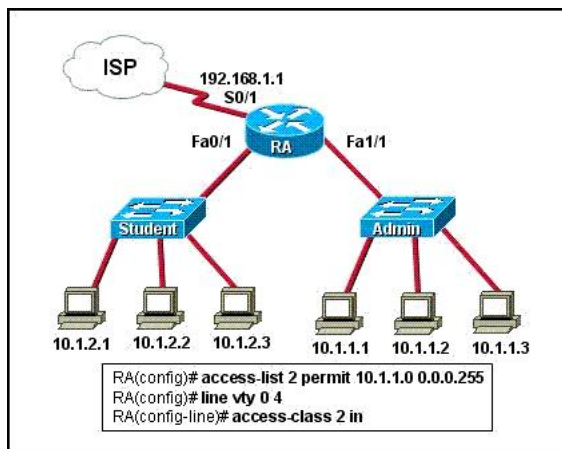
- access-list 10 permit 172.29.16.0 0.0.0.255
- access-list 10 permit 172.29.16.0 0.0.1.255
- access-list 10 permit 172.29.16.0 0.0.3.255
- access-list 10 permit 172.29.16.0 0.0.15.255
- access-list 10 permit 172.29.0.0 0.0.255.255

8. What are two reasons that a network administrator would use access lists?

(Choose two.)

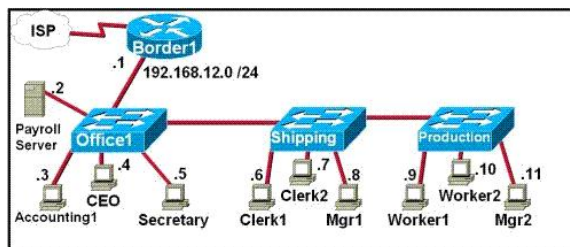
- A. to control vty access into a router
- B. to control broadcast traffic through a router
- C. to filter traffic as it passes through a router
- D. to filter traffic that originates from the router
- E. to replace passwords as a line of defense against security incursions

9. Refer to the exhibit. Why would the network administrator configure RA in this manner?



- A. to give students access to the Internet
- B. to prevent students from accessing the command prompt of RA
- C. to prevent administrators from accessing the console of RA
- D. to give administrators access to the Internet
- E. to prevent students from accessing the Internet
- F. to prevent students from accessing the Admin network

10. Refer to the exhibit. The FMJ manufacturing company is concerned about unauthorized access to the Payroll Server. The Accounting1, CEO, Mgr1, and Mgr2 workstations should be the only computers with access to the Payroll Server. What two technologies should be implemented to help prevent unauthorized access to the server? (Choose two.)



- A. access lists
- B. encrypted router passwords
- C. STP
- D. VLANs

E. VTP

F. wireless LANs



17.7 真题解答***

1. 解: ACE

题目问: 哪三个部分信息可以被扩展 ACL 用来过滤流量? 参照本章 17.3.1 节, 扩展 ACL 可以基于源地址、目标地址、协议 (如 TCP、UDP、IP 和 ICMP 等) 及端口号 (TCP 和 UDP 协议还涉及服务的端口号) 来过滤流量。

2. 解: DE

题目问: 参照图, RTB 路由器 S0/0 接口外出方向被配置了题目中的 ACL, 哪两个包路由到这个接口将被拒绝 (选两个)? 可以参照本章 17.3.1 节, 这个访问列表定义了两个语句, 在访问列表中匹配的秩序是从上到下, 如果匹配了某一句就执行操作, 然后退出访问列表; 如果没有就一直往下匹配, 在访问列表最后有一句隐含的是拒绝所有。所以不管怎么样都有一句是能被匹配的。在题中, 定义的第一句是拒绝从 192.168.15.32~ 192.168.15.47 发出的任何的 Telnet 的流量, 然后第二句定义的就是允许所有的 IP 流量。这里要知道 Telnet 使用的端口是 23, 正确答案是 D 和 E。

3. 解: A

题目问: 下面的访问列表有什么影响? 这是一个扩展的访问控制列表, 它可以基于源地址和目的地址进行匹配, 10.25.30.0 0.0.0.255 匹配的是源地址, 凡是在这个范围的都被匹配了, 也就是 10.25.30.*的地址都满足。而目的地址用的是 “any”, 表示 “任何”, 意思是 10.25.30.0/24 的地址范围内的任何 IP 都可以访问任何的网段。

4. 解: D

题目问: 一个访问控制列表被设计用来阻止 Accounting 部门的 HTTP 流量到达连接在 Holyoke 路由器上的 HR 服务器, 下面的哪一个 ACL 在 Chicopee 路由器的 e0 接口调用能完成此任务? 可以参照本章 17.3.2 节, 这里一定要先拒绝再允许, 如果把 permit ip any any 放在第一条, 永远执行不到第二条, 所有的流量都将被允许, 选项 A 和 B 都错。拒绝 172.16.16.0/24 去往 172.17.17.252/32 的 HTTP 的流量, HTTP 使用的是 TCP 的 80 端口, 题目中虽然没有指明 ACL 应用的方向 (或进或出), 源和目标地址不好确定, 但 80 端口对应的应该是 172.17.17.252/32, 选项 C 也错误。

5. 解:

这是一个拖拉题, 不用理会左边多出的一个选项。根据题的描述, 画出对应的拓扑如下图所示。右边第一个选项, 要求仅阻止连接在 Missouri 路由器 e0 接口的用户访问 Accounting 服务器, 应该选的是 “deny ip 192.168.35.16 0.0.0.15 host 192.168.35.66”。第二个选项, 要求阻止 Alabama 路由器上的一个用户访问 Accounting 服务器, 注意只要能阻止一个用户就可以了, 应该选的是 “deny ip 192.168.35.55 0.0.0.0 host 192.168.35.66”。第三个选项, 要求防止企业网络外的用户访问 Accounting 服务器, 访问列表最后隐含的是拒绝所有, 所以这里只要允许企业网络内的访问, 暗含的就是拒绝企业外的访问, 应该是 “permit ip 192.168.35.0 0.0.0.255 host 192.168.35.66”。



The Missouri branch office router is connected through its s0 interface to the Alabama Headquarters router s1 interface. The Alabama router has two LANs. Missouri users obtain Internet access through the Headquarters router. The network interfaces in the topology are addressed as follows: **Missouri:** e0 - 192.168.35.17/28; s0 - 192.168.35.33/28; **Alabama:** e0 - 192.168.35.49/28; e1 - 192.168.35.65/28; s1 - 192.168.35.34/28. The accounting server has the address of 192.168.35.66/28. Match the access list conditions on the left with the goals on the right. (Not all options on the left are used.)

deny ip 192.168.35.55 0.0.0.0 host 192.168.35.66

deny ip 192.168.35.16 0.0.0.15 host 192.168.35.66

permit ip any any

permit ip 192.168.35.0 0.0.0.255 host 192.168.35.66

deny ip 192.168.35.16 0.0.0.15 host 192.168.35.66

deny ip 192.168.35.55 0.0.0.0 host 192.168.35.66

permit ip 192.168.35.0 0.0.0.255 host 192.168.35.66

6. 解:

这是一个拖拉题，不用理会左边多出的多个选项。题目问，一个主机的 IP 地址是 192.168.125.34/27，拒绝该主机访问它自己子网外的所有主机，为了完成任务，从左边选项中选择内容来完成“access-list 100 deny protocol address mask any”列表中的 protocol、address 和 mask。正确的列表应该是“access-list 100 deny ip 192.168.125.34 0.0.0.0 any”。

A host with the address of 192.168.125.34 /27 needs to be denied access to all hosts outside its own subnet. To accomplish this, complete the command in brackets, [access-list 100 deny protocol address mask any], by dragging the appropriate options on the left to their correct placeholders on the right.

0.0.0.0

192.168.125.0

192.168.125.32

192.168.125.34

255.255.255.255

ip

tcp

udp

protocol

ip

address

192.168.125.34

mask

0.0.0.0

7. 解: C

题目问：图中的一个访问列表有四个语句，哪一个简单的列表能用一个语句组合成四个语句并有准确的相同效果？本题更像是路由汇总，一个单独的语句来匹配上面写出的四条 ACL，将 172.29.16.0/24、172.29.17.0/24、172.29.18.0/24、172.29.19.0/24 进行汇总，将它们的第 3 个 8 字节以二进制形成展开，相同的位作为它们的汇总条目，然后计算它们的掩码位数为多少，所以这四个条目汇总到一个条目为 172.29.16.0/22，掩码用通配符来写应该

是 0.0.3.255。

8. 解：AC

题目问：网络管理员使用 ACL 的两个原因是什么（选两个）？可以参照本章 17.4 节，在 VTY 线路下应用 ACL，可以控制从 VTY 线路进来的 Telnet 的流量。ACL 也可以过滤穿越一台路由器的流量，注意是穿越，ACL 对本路由器起源的流量不起作用。

9. 解：B

题目问：参照图，为什么网络管理员使用图中的方式配置路由器 RA？将 ACL 应用到 VTY 线路下，而且是 IN 的方向，表示凡是被此 ACL 允许的才能 Telnet 到该路由器。在 RA 上配置的是“permit 10.1.1.0 0.0.0.255”，允许 Admin 网段中的用户可以 Telnet 到路由器，隐含的 deny any 表示拒绝 Student 网段中的用户。

10. 解：AD

题目问：参照图，FMJ 制造公司关注到没有授权地访问 Payroll 服务器，仅允许 Accounting1、CEO、Mgr1 和 Mgr2 工作站可以访问 Payroll 服务器，哪两种技术可以被使用来阻止没有授权地访问服务器（选两个）？ACL 可以过滤三层的访问，如果 Payroll 服务器与图中的工作站在同一个 VLAN 中，它们之间的流量将不会经过路由器，ACL 也无法发生作用。可以通过 VLAN 技术，把 Payroll 服务器划到一个独立的 VLAN 中，再配置单臂路由，允许不同 VLAN 中的工作站可以访问 Payroll 服务器。进一步配置 ACL，限定每个 VLAN 中可以访问 Payroll 服务器的 IP 地址。

第 18 章

网络安全**

本章主要介绍网络中存在的安全威胁、减轻网络攻击的方法、配置基本的路由器安全、禁用路由器上不使用的端口和服务、使用 SDM 配置路由器的安全、管理路由器中的配置文件和 IOS、IDS 和 IPS 的功能介绍等内容。



18.1 网络安全介绍*

在网络的管理和实施中，网络安全变得越来越重要。企业需要开放网络来获取商机，企业也需要保护私有的、个人的和战略性的商业信息。本节主要介绍网络安全的重要性、一般存在的安全威胁、网络攻击的类型、一般防范网络攻击的技术和企业的安全策略。

18.1.1 网络安全的重要性*

计算机网络规模越来越大，在工作和生活中发挥着极其重要的作用。如果网络安全受到威胁，后果可能非常严重，如泄露隐私、信息被窃，甚至还会带来法律责任。一些潜在威胁始终不断发展变化，这使网络安全变得更有挑战性。在电子商务和互联网应用快速增长的今天，寻找网络孤立和开放两者之间的平衡是至关重要的。此外，移动商务和无线网络的发展需要网络安全解决方案能无缝集成，更加透明，更加灵活。

1. 日益增加的安全威胁

多年来，网络攻击的工具和方法不断演变。在 1985 年，攻击者必须有精密的电脑，还要具备编程和网络方面的知识。使用简陋工具和基本的攻击方法，一般人不具备这样的条件和能力的。可随着时间的推移，攻击的方法和工具大大改善，攻击者不再需要高水平的知识和技术，这有效地降低了攻击者的入门要求。以前不会参与计算机犯罪的人现在也能够做到了。随着威胁和攻击的演变，产生了一些名词和叫法：

- 白帽（White hat）。他们查找系统或网络的漏洞，然后向该系统业主报告这些漏洞，使业主能够进行加固。他们是反对破坏电脑系统的。白帽，一般侧重于保护信息系统，而黑帽则破坏系统。
- 黑客（Hacker）。历史上曾用来描述计算机编程专家。近年来，这个词是指那些未经授权试图获得访问资源或存在恶意企图的人。
- 黑帽（Black hat）。他们未获授权使用，通常为了个人或经济上的获益，利用他们的知识闯入电脑系统或网络系统。黑客是黑帽的一个例子。
- 破坏者（Cracker）。未经授权试图获得访问网络资源或存在恶意的企图。

- 盗用电话线路（Phreaker）。打入电话网络，通常是通过一个公用电话，免费地拨打长途电话。
- 垃圾邮件发送者（Spammer）。发送大量无用的电子邮件。垃圾邮件发送者经常使用病毒控制他人的电脑，并利用它们来传送其大量的信息。
- 钓鱼者（Phisher）。利用电子邮件或其他手段诱骗他人提供敏感资料，如信用卡号码或密码。

许多攻击者一般使用下面的 7 个步骤来获得信息和发动攻击。

- ① 侦察（Reconnaissance）。
- ② 列举信息。攻击者可以扩大监测网络流量，如数据包嗅探器，查找更多信息，如 FTP 服务器和邮件服务器的版本号等。
- ③ 获取用户信息。有时雇员选择的密码很容易被破解，有时雇员被欺骗而提供相关的敏感信息。
- ④ 升级特权。攻击者得到基本的访问权限之后，利用技能，以增加其网络的特权。
- ⑤ 收集更多的密码及机密。通过提升的访问权限，攻击者获得被保护更好、更敏感的信息。
- ⑥ 安装后门。后门提供了没有被发现的进入系统攻击方式。最常见的后门是一个开放的 TCP 或 UDP 端口。
- ⑦ 威胁系统。攻击者使用系统中获得的权限攻击网络中的其他主机。

2. 计算机中的攻击类型

计算机本身也极易受到攻击，典型的有：

- 内部滥用网络访问（Insider abuse of network access）；
- 病毒（Virus）；
- 拒绝服务（Denial of Service）；
- 滥用无线网络（Abuse of Wireless Network）；
- 系统渗透（System Penetration）；
- 密码嗅探（Password Sniffing）。

18.1.2 一般的安全威胁*

讨论网络安全，要考虑 3 方面的因素：弱点、威胁和攻击。弱点是所有网络和网络设备固有的，包括路由器、交换机、台式机、服务器，甚至安全设备。威胁有使用各种工具、脚本和程序对网络和网络设备发动攻击。在通常情况下，易受到攻击的是终端设备，如服务器和台式电脑。有 3 个方面的漏洞或薄弱环节。

- 技术弱点：协议存在的弱点、操作系统存在的弱点、网络设备存在的弱点。
- 配置弱点：用户账号设置不安全、系统账号密码简单、不安全的产品默认设置、网络服务配置有误、网络设备配置有误等。
- 安全策略弱点。

网络威胁除了有来自无形的攻击，也有来自有形的威胁，包括：硬件受到物理损坏、环境温度和湿度变化、电力保障、布线符合规范等。

网络威胁主要有 4 个类别：

- 非结构化的威胁，大多数是缺乏经验的个人，使用容易找到的黑客工具来发动攻击。
- 结构化的威胁，一般是有组织的团体、富有经验的攻击者发动的攻击。
- 外部威胁，从组织外部发动的攻击。
- 内部威胁，来自组织内部的攻击。

社会工程学是另一种不同的攻击手段，也就是通常特务所做的工作。

18.1.3 网络攻击类型**

主要有 4 种类型的攻击：

(1) 侦察 (Reconnaissance)

侦察是未经授权发现和扫描系统、服务或漏洞。它也被称为信息收集，在大多数情况下，它是另一种类型攻击的先导。侦察攻击包括：

- Internet Information Queries (Internet 信息查询)，使用网络搜索功能，获取到更多的信息。
- Ping Sweeps (Ping 扫描)，通过使用 ping 命令检测目标主机是否在线、安装的操作系统等。
- Port Scans (端口扫描)，探测目标主机开放的端口，判断目标主机开放的服务，找到攻击弱点。
- Packet Sniffers (包嗅探)，捕获数据包，从中获取更多的有用信息。

(2) 访问 (Access)

系统访问是入侵者有能力访问没有账户和密码的设备。进入或访问系统通常包括运行黑客软件、脚本或工具，利用一个已知系统或应用程序弱点发动攻击。访问攻击包括：

- Password Attacks (密码攻击)，典型使用的是暴力破解密码。
- Trust Exploitation (信任利用)，利用操作系统的特点，比如 Windows 的信任机制。
- Port Redirection (端口重定向)，使用端口重定向，绕开安全设备的限制，达到攻击的目的。
- Man-in-the-Middle Attack (中间人攻击)，攻击者在源和目标之间截获数据包，发动攻击。

(3) 拒绝服务 (Denial of Service, 简称 DoS)

攻击者想办法让目标机器停止提供服务或资源访问，这些资源包括磁盘空间、内存、进程甚至网络带宽，从而阻止正常用户的访问。拒绝服务攻击包括：

- Ping of Death (Ping 死)，Ping 死攻击是利用 ICMP 协议的一种碎片攻击。主要用在过去，攻击者发送一个长度超过 65535 字节的 Echo Request 数据包，目标主机在重组分片的时候会造成事先分配的 65535 字节缓冲区溢出，系统通常会崩溃或挂起。现在多数操作系统的主机都有防范 Ping of Death 的功能。
- SYN Flood (SYN 洪水)，SYN Flood 是当前最流行的 DoS (拒绝服务攻击) 与 DDoS (Distributed DoS, 分布式拒绝服务攻击) 的方式之一，这是一种利用 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，从而使得被攻击方资源耗尽 (CPU 满负荷或内存不足) 的攻击方式。
- DDoS，简单地讲，拒绝服务就是用超出被攻击目标设备处理能力的海量数据包消耗可用系统、带宽资源，致使服务瘫痪的一种攻击手段。在早期，拒绝服务攻击主要

是针对处理能力比较弱的单机，如 PC 或窄带宽连接的网站，对拥有高带宽连接、高性能设备的网站影响不大。但伴随着 DDoS 的出现，高端网站高枕无忧的局面不复存在。DDoS 的实现是借助数百甚至数千台被植入攻击守护进程的攻击主机同时发起的集团作战行为。因此，分布式拒绝服务也被称为“洪水攻击”。

- **Smurf Attack (Smurf 攻击)**，Smurf 攻击可能是最早的分布式 DoS 攻击的形式。攻击者先使用扫描程序搜索一些允许广播包的路由器，找到这种路由器以后，攻击者就可以着手攻击目标了。这种路由器有一个特性，在这个网段内的每台机器都会对 ping 广播包回应一个包，所以，如果这个网段内有 100 台机器，一台机器发一个 ping 广播包，将有 100 个包回复给这台机器。攻击者向这种路由器发送一些经过伪造的报文，包头上的地址伪造为要攻击计算机的地址，这样通过不停地发送这些伪造的 ping 广播包，被攻击计算机收到的将是数以百倍计的报文，很快被攻击的计算机就会被淹没在这种洪水般的报文中，对其他的正常请求失去反应能力。

(4) 蠕虫、病毒和特洛伊木马 (Worms、Viruses and Trojan Horses)

18.1.4 一般防范攻击的技术*

对攻击的防范可以是基于主机的，也可以是基于网络安全设备的。

1. 基于主机的防范技术

- **更改默认配置**。当操作系统被安装后，安全设置采用的是默认值。在大多数情况下，这个级别的安全性是不够的。有一些简单的应采取的步骤适用于大多数的操作系统，即立即更改默认的用户名和密码，对资源访问进行授权，禁用不必要的服务和应用程序。
- **安装防病毒软件**。主机安装防病毒软件可防止已知病毒。防病毒软件可以侦测到大部分的病毒和许多特洛伊木马，并防止它们在网络中传播。
- **安装个人防火墙**。将防火墙安装在个人计算机上，用来阻止攻击。
- **安装补丁**。从操作系统和应用程序厂商处下载修补程序，也称为补丁程序，主要用来修复操作系统和应用程序出现的漏洞。

2. IDS 和 IPS

入侵检测系统 (Intrusion Detection System, IDS) 检测网络攻击并发送日志记录到管理控制台。入侵防御系统 (Intrusion Prevention System, IPS) 防止攻击网络，除了检测外还提供下列积极防御的机制：阻止、停止检测到的攻击；预防：使系统今后免受一个恶意来源的攻击。IDS 和 IPS 的比较如表 18-1-1 所示。

表 18-1-1 IDS和IPS的比较

	IDS	IPS
能否检测攻击，并发送日志和报警	能	能
能否主动防御	不能，只能发送消息，提醒相关的设备采取措施	能，IPS 可以主动阻止恶意的流量，甚至断开网络连接
在网络中部署的位置	一般是旁路	一般是串接

可以配置网络级或主机级的 IDS 和 IPS，或者网络级和主机级都配置，以提供最大的保护。如果是基于主机的则称为基于主机的入侵检测系统 (Host-based Intrusion Detection

System, HIDS) 和基于主机的入侵防御系统 (Host-based Intrusion Prevention System, HIPS)。

HIPS 软件必须被安装在每个主机、服务器或台式机中, 用来监测活动任务和保护主机。这个软件被称为代理软件, 代理软件执行入侵检测分析及预防, 代理软件还发送日志和警报到集中管理或策略服务器。

HIPS 的优势是可以监测操作系统的进程和保护关键系统资源, 包括可能只存在特定主机上的文件。这意味着, 当一些外部的进程 (包括一些隐藏的黑客后门程序) 尝试修改系统文件时, 它可以通知网络管理者。

3. 一般的安全设备和应用程序

规划一个网络时, 安全是首先要考虑的。在过去, 一提到网络安全设备, 想到的就是防火墙。单纯的防火墙已不能给网络足够的保护, 典型的网络安全需要综合防火墙、入侵预防和 VPN 的功能。

下面介绍一些相关的网络安全设备和应用程序, 在 CCNP 课程中可以更深入地学习。

- NAC (Network Admission Control), 提供基于角色的方法阻止没有授权的网络访问。思科有专门的 NAC 设备。
- ISR (Integrated Services Router, 集成服务路由器), 思科使用 IOS 软件提供用户所需要的很多安全方法, 思科 IOS 软件内置了防火墙、IPSec、SSL VPN 和 IPS 服务。
- ASA (Adaptive Security Appliance, 自适应安全设备), 早先保护网络将部署 PIX 防火墙, 后来 PIX 防火墙集成了更多的安全特性, 叫做 ASA, 也就是说, ASA 是 PIX 的升级版, 功能比 PIX 更全、更强。ASA 集防火墙、语音安全、SSL VPN、IPSec VPN、IPS 和安全内容服务于一身。
- IPS, 在大型网络中, 可以部署在线的入侵防御系统用来识别、区分和停止网络中的恶意流量。
- CSA (Cisco Security Agent, 思科安全代理), CSA 是一款软件, 用来对服务器、台式机和 POS (Point-Of-Service, 服务点) 计算机系统提供保护。

18.1.5 网络安全车轮 (Network Security Wheel) *

很多安全事件发生的原因是因为系统管理员不执行现有的对策, 而攻击者或心怀不满的雇员利用了这点疏忽, 因此, 问题不在于只是确认一个技术漏洞的存在, 而且要找到对策, 这也是关键, 以验证该对策正在工作并且工作正常。

使用安全车轮协助检验安全策略, 已被证明是一种有效的办法。在安全车轮处理中, 首先要建立一个安全策略, 使应用得到保护。安全策略包括以下内容:

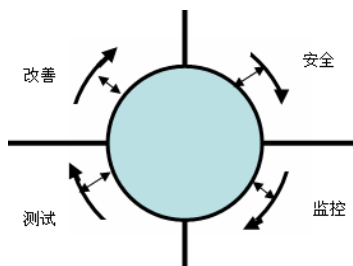


图 18-1-1 网络安全车轮

- 确定组织的安全目标;
- 记录需要得到保护的资源;
- 识别网络基础设施;
- 确定关键需要保护的资源, 如研究和开发、财务和人力资源, 也就是所谓的风险分析。

安全策略是枢纽, 基于安全车轮的 4 个步骤是: 安全、监控、测试和改善, 如图 18-1-1 所示。

第 1 步: 安全 (Secure)。使用威胁防御、安全连接、

状态检测和包过滤来保护网络安全。

第 2 步：监控（Monitor）。包括审计主机级别的日志文件、使用入侵检测设备、自动侦测入侵。网络监控的一个额外的好处是核查已配置的安全车轮第 1 步实施的保护措施是否工作正常。

第 3 步：测试（Test）。积极主动地进行测试，具体来说，检查第 1 步安全解决方案的实施，检查和验证第 2 步系统审计和入侵检测方法的实施。用一些攻击手段周期性地进行测试。

第 4 步：改善（Improve）。安全车轮的改善阶段包括分析监控期间和测试阶段收集的数据。这个分析有助于制定和实施改善机制，增强安全策略的效果，重新调整第 1 步。为了保护网络尽可能安全，周期的安全车轮必须不断重复，因为网络脆弱性和新的风险不断出现。



18.2 路由器的安全**

在任何安全部署中，路由器的安全都是一个关键要素。路由器在网络中主要执行通告网络，提供不同网络间的互访，并控制网络间访问的功能，往往是网络攻击的目标。

就像前面介绍过的攻击方法，路由器也经常受到各种各样的攻击，网络管理员不可能使用单一的方法来防范各种攻击。本节介绍一些方法来加强路由器的安全，包括：加强路由器的密码安全、限制远程访问、记录日志、禁用有弱点的服务和不使用的接口、加强路由协议的安全、控制和过滤网络流量等。

18.2.1 密码安全*

对路由器最直接的攻击方法就是获取路由器的密码。保护路由器密码安全的方法包括：

- 设置一个复杂的密码，比如设成“PaSSord_!@3”，而不要设成“password”或者简单的单词、电话号码或生日等。
- 对配置文件中的密码实行加密，使用“service password-encryption”命令对所有密码进行加密。
- 对 enable 密码使用“enable secret”，而不要使用“enable password”。
- 限制密码的最小长度，使用“Router(config)#security passwords min-length 10”命令，把密码的最小长度限制到 10 位。
- 加强密码的存放安全，不要记在纸上或随意告诉别人。
- 加强对路由器存放位置的保护，不允许一般人随便接触，以免他们使用路由器的密码恢复技术来重置路由器的密码。

18.2.2 限制远程访问**

攻击者可以尝试使用暴力破解密码来获取路由器远程登录的密码，或使用密码嗅探工具来捕获他人的明文密码。可以通过下面两种方法来限制对路由器的远程访问和密码泄露。

1. 限制对 VTY 终端的访问

在默认情况下，路由器允许来自所有 IP 地址的远程登录。可以使用下面的命令来限制只允许网络管理员从远程登录路由器（斜体部分是注释）。


```
Router(config)#access-list 1 permit 192.168.1.3      192.168.1.3 是网络管理员的 IP 地址。
Router(config)#line vty 0 4
Router(config-line)#access-class 1 in
```

这里特别值得提醒的是，很多工程师通过在路由器的所有接口下挂接 ACL 来实现只有合法的 IP 地址才可以访问路由器的 TCP 的 23 号端口，这种方法是非常不可取的，因为在路由器接口下挂接 ACL，路由器需要对所有进入的数据包都进行检查，这会增加路由器的负担；还要注意不能影响到合法的流量，包括正常的路由协议包等；路由器往往不止一个接口，也不止一个 IP 地址，那就需要在所有接口下，针对所有 IP 地址都进行限制。

2. 使用 SSH 替代 Telnet

Telnet 使用明文密码，在网络上传输是非常不安全的，尤其是跨越 Internet 的访问。对网络的远程访问推荐使用 SSH 技术，SSH 是英文 Secure Shell 的简写。通过使用 SSH，可以对所有传输的数据进行加密，这样“中间人”攻击方式就不可能实现了，捕获的数据包也是 RSA 加密后的数据包。

使用 SSH 要进行服务器端和客户端配置。

(1) 配置 SSH 服务器端

启动路由器 R1，把路由器 R1 配置成 SSH 服务器端，步骤如下：

① 准备工作。给路由器 R1 配置一个 IP 地址：

```
Router(config)#int fa 0/0
Router(config-if)#ip add 192.168.1.100 255.255.255.0
Router(config-if)#no shut
```

② 配置路由器的名字。路由器的默认名字一定要改变，配置如下：

```
Router(config)#host R1
```

③ 配置路由器的域名。路由器的域名一定要配置，随便配置一个域名就可以了，配置如下：

```
Router(config)#ip domain-name test.com
```

④ 产生非对称密钥。使用“crypto key generate rsa”命令产生非对称密钥，密钥的名字是 R1.test.com。然后询问密钥的长度，可以从 360 到 2048，这里输入 1024。稍后路由器提示“SSH 1.99 has been enabled”，表示路由器现在可以支持 SSH 了。密钥的产生过程、输入密钥的位数、路由器的提示等如下所示：

```
R1(config)#crypto key generate rsa
The name for the keys will be: R1.test.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
R1(config)#
*Mar 1 01:55:10.263: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

⑤ 配置 VTY 用户使用本地验证，验证的方式是 SSH，配置如下（斜体部分是注释）：

```
R1(config)#username test secret cisco!##%&      创建一个用户 test，使用加密的密码 cisco!##%&。
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
允许使用 SSH 登录，其他的验证方式比如 Telnet 都被禁用，也可以允许使用多种验证方式，比如 transport
input ssh telnet。
R1(config-line)#login local                      使用路由器本地的用户验证。
```

⑥ 调整 SSH。第②～⑤ 步是必须配置的，此外还可以配置一些可选项来调整 SSH。配置如下（斜体部分是注释）：

```
R1(config)#ip ssh time-out 15  SSH 窗口的超时时间。比如提示输入密码，如果用户迟疑 15 秒钟，
                               然后再输入，则认为已经超时，需刷新后重新输入。
R1(config)#ip ssh authentication-retries 3  每次 SSH 连接允许尝试的次数，三次登录失败后，
                                             需再次连接 SSH。
```

（2）配置 SSH 客户端

由于很多操作系统默认不提供 SSH 客户端功能，需要安装额外的 SSH 客户端软件，这里以 SecureCRT 软件为例讲述 SSH 客户端的配置。步骤如下：

① 安装 SecureCRT 软件。SecureCRT 软件在 CCNANEW.rar 压缩包中，该软件的安装比较简单，这里省略。

② 配置 SecureCRT。单击“文件”菜单→“连接”，打开“连接”窗口，如图 18-2-1 所示。

单击“连接”窗口工具栏中左起的第 3 个图标“New Session”，打开“新建会话向导”对话框，如图 18-2-2 所示，在“协议”栏中，选择“SSH1”。单击“下一步”按钮继续。

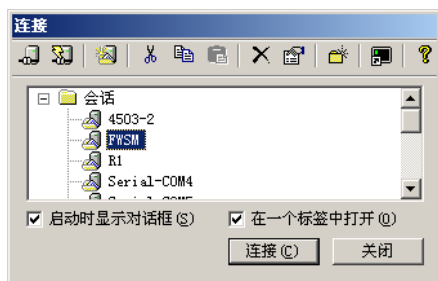


图 18-2-1 “连接”窗口



图 18-2-2 选择协议

新建会话向导询问远程主机的名称和 IP 地址是什么？如图 18-2-3 所示进行填写，在“主机名”栏中输入路由器 R1 的 IP 地址“192.168.1.100”；“端口”号中保持默认的“22”，SSH 使用的是 TCP 协议 22 号端口；“防火墙”栏中保持默认的“无”；“用户名”栏中填入在路由器中添加的用户名“test”。单击“下一步”按钮继续。

新建会话向导会询问会话名称，如图 18-2-4 所示，这里保持默认或填入一个更直观的名称，比如“R1”。单击“完成”按钮，完成新连接的添加。



图 18-2-3 填入远程主机信息

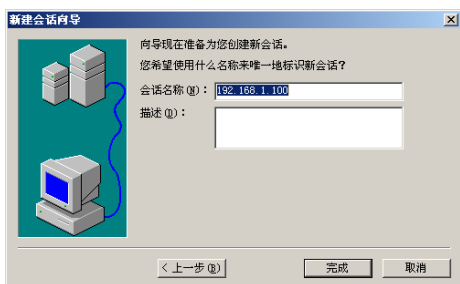


图 18-2-4 填入会话名称

③ 编辑连接属性。步骤②中添加的新连接，默认使用压缩形式，可是路由器端不支持压缩。选中“连接”窗口中新建的“192.168.1.100”，单击工具栏中左起第 8 个图标“properties”，

修改连接的属性，如图 18-2-5 所示。

在打开的“会话选项”窗口中，如图 18-2-6 所示，在左侧栏中选中“高级”，在右侧的压缩栏中选择“无”，单击“确定”按钮返回。

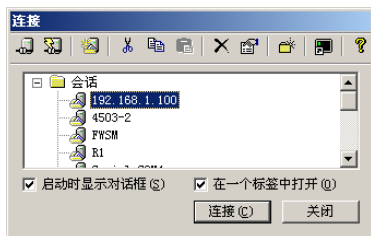


图 18-2-5 编辑连接属性

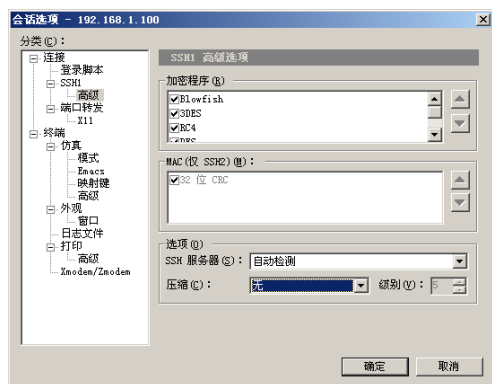


图 18-2-6 编辑会话选项

单击图 18-2-5 中的“连接”按钮，弹出如图 18-2-7 所示的对话框，在对话框中的“口令”栏中输入 test 用户的密码“cisco!#%&”，单击“确定”按钮，SecureCRT 成功通过 SSH 连接到路由器 R1。若测试失败，请确认测试计算机可以访问 192.168.1.100。

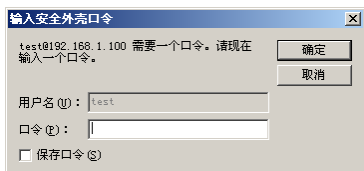


图 18-2-7 输入口令

18.2.3 记录日志**

日志可以用来验证路由器工作是否正常，也可以用来判断路由器是否受到威胁。在某些场合，日志还能显示路由器或受保护的网络受到的攻击或探测。

用户平时通过 Console 口对路由器进行配置时，经常可以看到下面的提示消息：

```
R1(config-if)#no shut
R1(config-if)#
*Mar 1 04:03:12.246: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
*Mar 1 04:03:13.250: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1,
changed state to up
```

可是通过远程登录后，却看不到这样的提示了。尤其是路由器或交换机产生 IP 地址冲突、MAC 地址表不稳定时错误提示信息，从远程登录时也不会显示，这就给网管发现问题带来很大的不便。还有的读者试图在虚拟终端（VTY）上执行 debug 命令，结果什么信息也没有显示。出现上述情况的原因是，虚拟终端默认是关闭监控的，登录远程终端后可以使用下面的命令打开终端监控功能：

```
Router# terminal monitor
```

使用下面的命令关闭终端监控功能：

```
Router# terminal no monitor
```

为了打开或关闭日志消息，用户可以输入“logging on”命令或者“no logging on”命令。工程师不可能 24 小时盯着显示器的屏幕来查看路由器或交换机的提示信息或日志，可以配置日志缓存功能，命令如下：

```
R1(config)#logging buffered ?
<0-7> Logging severity level
```

```
<4096-2147483647> Logging buffer size
alerts          Immediate action needed          (severity=1)
critical        Critical conditions            (severity=2)
debugging       Debugging messages              (severity=7)
emergencies     System is unusable                (severity=0)
errors          Error conditions                  (severity=3)
filtered        Enable filtered logging
informational    Informational messages                    (severity=6)
notifications    Normal but significant conditions (severity=5)
warnings        Warning conditions                      (severity=4)
xml             Enable logging in XML to XML logging buffer
<cr>
```

```
R1(config)#logging buffered informational
```

logging buffered 可以把日志消息发送到缓存中,后面的 informational 是发送日志的消息级别,相当于级别 6,也可以直接输入数字 6。如果对级别 6 的消息进行记录,路由器将记录比级别 6 高的所有消息,也就是记录 0, 1, 2, 3, 4, 5, 6 级的所有消息。路由器上支持 8 个级别的记录,从 0 到 7,如果记录级别为 7 (调试信息),路由器将记录所有的信息。

为了便于查看事件发生的时间,一般使用下面的命令把日志消息打上时间戳:

```
R1(config)# service timestamps debug datetime msec      对 debug 消息打上时间戳,时间准确到毫秒。
R1(config)# service timestamps log datetime msec        对 log 消息打上时间戳。
```

可以使用“show logging”命令查看缓存中的记录。但路由器的缓存空间毕竟很有限,且断电或重启后,缓存中的所有日志都会丢失。一般的做法是配置一台专门的日志服务器,把路由器或交换机的日志发送到日志服务器。有关日志服务器的配置,不在 CCNA 考试的范围内,感兴趣的读者可以查阅相关资料。

18.2.4 禁用不需要的服务或端口*

思科路由器支持大量的服务,如 CDP、TCP small servers、UDP small servers、Finger、HTTP server、BOOTP server、Proxy ARP、IP directed broadcast 等。而大量服务一般是不需要的,开着这些服务,将给路由器带来资源浪费,并可能引起攻击,给路由器带来安全隐患。关闭这些服务是非常有必要的,比如使用“no cdp run”命令关闭 CDP 协议,使用“no ip http server”命令关闭 HTTP 服务。

很多管理员并不知道路由器上有哪些默认打开的服务需要被关闭,且使用命令行的方式关闭所有不使用的服务非常烦琐。思科 AutoSecure 使用一个单一的命令停用不必要的系统进程和服务,消除潜在的安全威胁。可以在特权 Exec 的模式下使用 AutoSecure,有两种模式:

- 交互模式,这种模式会提示选择启用或禁用服务和其他的安全功能。这是默认模式。
- 非交互模式,这个模式自动执行思科推荐的安全设置。

思科交互模式的 AutoSecure 会问若干项目,包括:接口指定、旗帜消息、密码设置、SSH 配置、IOS 防火墙特性集等。

下面是采用非交互模式执行的 AutoSecure。

```
R1#auto secure no-interact
--- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
```

```
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
```

```
Securing Management plane services...
```

```
Disabling service finger
```

```
(省略的部分输出)
```

```
Disabling gratuitous arp
```

```
Configuring interface specific AutoSecure services
```

```
Disabling the following ip services on all interfaces:
```

```
no ip redirects
no ip proxy-arp
no ip unreachableables
no ip directed-broadcast
no ip mask-reply
```

```
Securing Forwarding plane services...
```

```
Enabling CEF (This might impact the memory requirements for your platf
```

```
This is the configuration generated:
```

```
no service finger
no service pad
no service udp-small-servers
(省略的部分输出)
interface FastEthernet0/0
no ip redirects
no ip proxy-arp
no ip unreachableables
no ip directed-broadcast
no ip mask-reply
(省略的部分输出)
no ip mask-reply
ip cef
!
end
```

```
Applying the config generated to running-config
```

```
R1#
```

从上面的输出中可以看到，在路由器上仅使用一个非交互式的“auto secure no-interact”命令，产生了很多相关的安全配置，禁用了很多思科默认启用的服务。



18.3 SDM *

SDM (Security Device Manager, 安全设备管理) 是基于 Cisco IOS Software 的路由器开发的一种直观的 Web 设备管理工具。它能够通过智能向导简化路由器和安全配置，使用户不需要了解命令行界面 (CLI) 就能快速、容易地部署配置和监控思科路由器。许多 Cisco 路由器和 Cisco IOS Software 版本均可以支持 Cisco SDM。本节主要介绍 SDM 的使用。

18.3.1 SDM 的关键特性

(1) 易用性和内置应用智能

利用 Cisco SDM，用户不但能轻松地在 Cisco 路由器上配置路由、交换、安全和服务质

量 (QoS) 服务, 还能通过性能监控进行主动管理。现在 Cisco SDM 用户可以远程配置和监控 Cisco 路由器而不再需要使用 Cisco IOS Software CLI。Cisco SDM 图形化界面能够帮助非专家型用户完成日常操作, 提供易于使用的智能向导, 自动执行路由器安全管理并通过全面的在线帮助和指导给予用户帮助。Cisco SDM 智能向导指导用户通过系统地配置 LAN、WLAN 和 WAN 接口、防火墙、入侵防御系统 (IPS) 和 IP Security (IPSec) VPN 来逐步完成路由器和安全配置工作。Cisco SDM 智能向导能够以智能方式检测到错误配置并提出修复建议, 比如, 如果 WAN 接口是 DHCP 获取地址的, 则允许 DHCP 的流量通过防火墙。SDM 除了提供详细的步骤外, 内嵌的在线帮助还提供了相应的背景信息。

(2) 集成式安全配置

部署新的路由器时, 可以利用国际计算机安全协会 (ICSA) 和 Cisco 技术支持中心 (TAC) 推荐的最佳实践来使用 Cisco SDM 快速配置 Cisco IOS Software 防火墙。先进的防火墙向导可以配置安全要求高、中、低的应用程序防火墙。Cisco SDM 用户可以配置最强的 VPN 默认值, 并自动执行安全审计。此外, Cisco SDM 用户可以执行防火墙的一步路由器锁定, 并通过一步 VPN 快速部署安全站点到站点连接。Cisco 推荐的与 Cisco SDM 捆绑在一起的 IPS 签名表可以快速部署蠕虫、病毒和协议攻击抵御系统。通过 Cisco SDM 网络准入控制 (NAC) 向导, 可以简单、快速地将 NAC 和客户机安全状态管理集成到现有的网络基础架构中。

(3) 路由器配置

除安全配置外, Cisco SDM 还能帮助用户快速、轻松地执行路由器服务配置, 例如: LAN、WLAN 和 WAN 接口配置、动态路由、DHCP 服务器、QoS 策略等。利用 LAN 配置向导, 用户不但能为以太网接口分配 IP 地址和子网掩码, 还能启动或禁用 DHCP 服务器。利用 WAN 配置向导, 用户可以为 WAN 和互联网接入配置 xDSL、T1/E1、以太网和 ISDN 接口。另外, 对于串行连接, 用户还可以实施帧中继、点对点协议 (PPP) 和高级数据链路控制 (HDLC) 封装。不仅如此, Cisco SDM 还允许配置静态路由和通用动态路由协议, 例如: “开放最短路径优先” (OSPF)、“路由信息协议” (RIP) 第 2 版和“增强型内部网关路由选择协议” (EIGRP)。现在利用 Cisco SDM, 可以轻松地将 QoS 策略应用到任何 WAN 或 VPN 通道接口。QoS 策略向导能够自动执行 QoS 策略的 Cisco 体系结构原则, 以便有效区分实时应用 (语音或视频)、关键业务应用流量及其他网络流量 (Web 电子邮件等)。借助 Cisco SDM 中基于网络的应用程序识别监控, 用户能够以可视方式实时检查应用层流量, 并不断分析 QoS 策略对各种应用流量的影响。

(4) 监控和故障排除

在监控模式下, Cisco SDM 能够以图形方式快速显示重要路由器资源的状态和性能数据, 例如接口状态 (正常或不正常)、CPU 和内存使用等。Cisco SDM 可以利用路由器上的集成式路由和安全特性深入诊断 WAN 和 VPN 连接, 并及时排除故障。Cisco SDM 监控模式不但允许用户检查被 Cisco IOS Software 防火墙拒绝的网络访问企图次数, 还可以提供访问防火墙记录。不仅如此, 用户还可以监控详细的 VPN 状态信息, 例如: IPSec 通道加密或解密的包数, 以及 Easy VPN 客户机连接细节。

(5) 降低成本

Cisco SDM 适合那些对设备部署和网络管理成本敏感, 但缺少高技能技术人员的企业分支办公室和中小型商业机构。利用 SDM 用户能够轻松地实施路由器安全和网络配置。

Cisco SDM 生成的 Cisco IOS Software 配置已通过 Cisco TAC 批准。Cisco SDM 能够通过内置配置检查、专家配置编辑器和有意义的默认值，提高网络和安全管理员的生产率。另外，Cisco SDM 特性还能减少配置出错机会，大大提高网络可靠性。

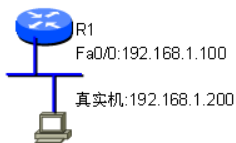


图 18-3-1 SDM 实验拓扑

18.3.2 配置 SDM

CCNA 模拟器中的路由器 R1、R2、R3 均支持 SDM。接下来的部分结合图 18-3-1，在真实机上通过 SDM 完成对路由器的管理。

1. 配置路由器支持 SDM

路由器 R1 的配置如下（斜体部分是注释）：

```
R1#conf t
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.100 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#ip http server
SDM 通过使用 IE 浏览器来配置路由器，所以路由器必须要启用 http，如果担心 http 不安全，可以使用 “ip
http secure-server” 命令，开启 https 支持。
R1(config)#ip http authentication local
HTTP 的验证方式是本地，即使用路由器上的用户名和密码来验证，如果不配置 HTTP 验证，将使用路由器的特
权密码验证，如果没有配置特权密码，SDM 的访问将不需要密码，那是非常不安全的，使用中的设备一定要使用验证。
R1(config)#user test privilege 15 secret test!##%
需要权限 15 的用户才能配置 SDM。
R1(config)#line vty 0 4
不是 SDM 必需的步骤，但考虑到路由器的远程命令行访问，可以配置 VTY 的访问方式作为备用。下面的两个步
骤也不是必需的步骤。
R1(config-line)#login local
R1(config-line)#transport input ssh telnet 允许 SSH 和 Telnet 的方式访问远程终端。
```

2. 在计算机上安装 SDM 软件

CCNANEW.rar 中提供了 SDM-V241.zip 和 SDM-V241-zh 中文版.zip 两个文件，读者可以选择安装中文版或英文版，本书以中文版的使用为例。解压缩 SDM-V241-zh 中文版.zip 到某个文件夹下，双击此文件夹中的“setup.exe”文件进行安装。如果读者的计算机上不具备 Java 环境，会弹出如图 18-3-2 所示的窗口，单击“是”按钮，向导将访问 Java 网站，进行下载。考虑到网速的原因，这里单击“否”按钮，记得安装完 SDM 后，一定要安装 CCNANEW.rar 中的 Java 文件“j2re-1_4_2_12-windows-i586-p.exe”。



图 18-3-2 没有安装 Java 提示

在如图 18-3-3 所示的 SDM 安装向导中单击“下一步”按钮继续，在接下来的窗口中接收许可证协议，继续单击“下一步”按钮。

SDM 安装向导询问安装选项，如图 18-3-4 所示，这里选择“本计算机”，单击“下一步”按钮继续。接下来，SDM 安装向导询问安装的路径，保持默认就可以了。最后，完成 SDM 的安装。如果没有安装 Java，再继续安装 Java。



图 18-3-3 SDM 安装向导

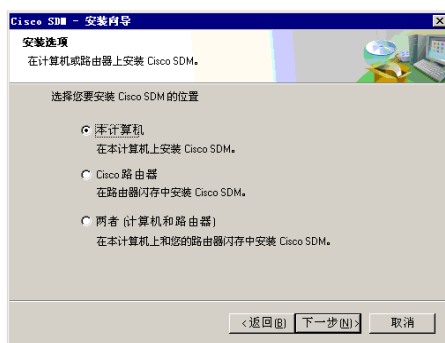


图 18-3-4 SDM 安装选项

3. 使用 SDM 查看路由器信息

SDM 安装完成后，双击桌面上的“Cisco SDM (Chinese Edition)”快捷图标，打开如图 18-3-5 所示的窗口，在地址栏中输入“192.168.1.100”，单击“启动”按钮。

弹出如图 18-3-6 所示的 SDM 验证窗口，在“用户名”栏中输入“test”，在“密码”栏中输入“test!#%&”，单击“确定”按钮。

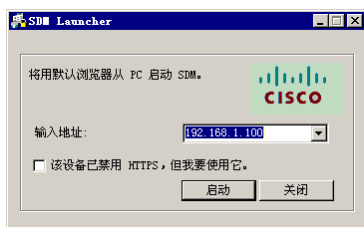


图 18-3-5 SDM 连接

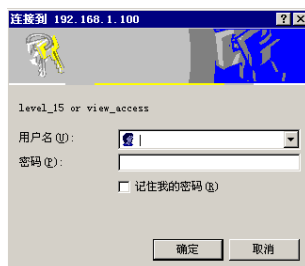


图 18-3-6 SDM 验证

弹出“警告 - 安全”窗口，如图 18-3-7 所示，单击“是”按钮继续，如果不想每次运行 SDM 时都出现这个警告窗口，可以单击“总是有效”按钮。

再次弹出身份验证窗口，如图 18-3-8 所示，在“用户名”栏中输入“test”，在“口令”栏中输入“test!#%&”，单击“是”按钮。

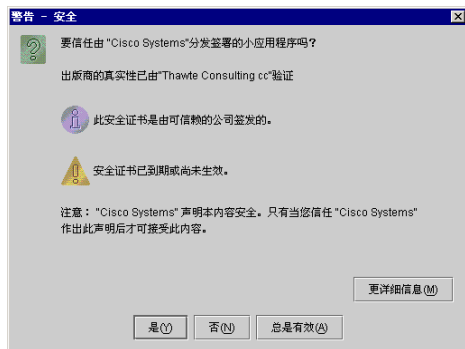


图 18-3-7 安全警告

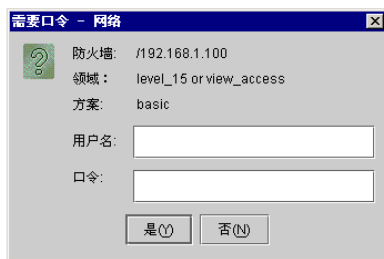


图 18-3-8 再次验证身份

有些操作系统的 IE 浏览器可能打开的是一个代码窗口，此时需要修改 IE 浏览器的安全设置。单击 IE 浏览器的“工具”→“Internet 选项”，打开“Internet 选项”窗口，如图 18-3-9

所示, 选择“高级”标签, 选中“允许活动内容在我的计算机上的文件中运行”复选框, 单击“确定”按钮返回。有的系统需要单击 IE 浏览器的“工具”→“Internet 选项”, 打开“Internet 选项”中的“安全”标签, 把安全级别降到中低。关闭 IE 浏览器窗口, 重新启动 SDM。

SDM 开始从路由器中装入当前配置, 稍后打开路由器的 SDM 管理界面, 如图 18-3-10 所示。从图中可以看到路由器的硬件和软件、接口和连接、防火墙策略、VPN、路由和入侵检测等信息。还可以单击“查看运行配置”按钮, 查看当前路由器的配置。

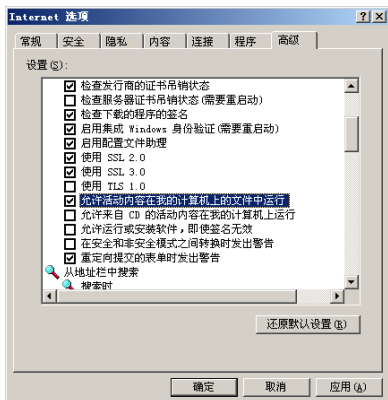


图 18-3-9 修改 IE 的高级选项



图 18-3-10 SDM 管理界面

4. 使用 SDM 配置路由器

使用 SDM 可以对路由器中的很多服务和功能进行配置, 单击图 18-3-10 所示工具栏中的“配置”图标, 打开如图 18-3-11 所示的配置窗口, 从左侧栏中选择相应的功能进行配置。后面章节介绍了使用 SDM 配置站点到站点 VPN。虽然 CCNA 考试中并不涉及 SDM 的使用, 但 SDM 在实际工程中却相当有用, 尤其是那些对思科命令行不是很熟悉的使用者。

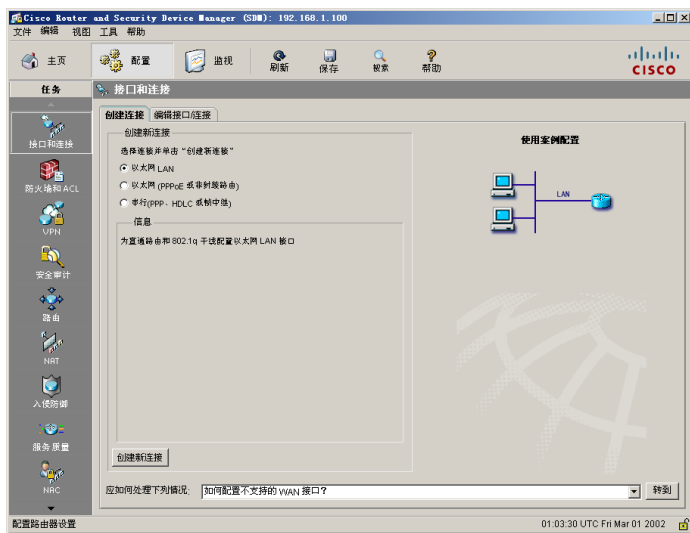


图 18-3-11 SDM 配置窗口



18.4 路由器的文件管理 *

路由器中的文件包括操作系统（IOS）和配置文件（startup-config），本节介绍思科路由器中 IOS 文件和配置文件的管理及维护。

18.4.1 IOS 文件管理

IOS 文件管理包括备份 IOS、升级 IOS 和恢复 IOS。

1. 备份 IOS 文件

出于安全方面的考虑，可以对路由器的 IOS 文件进行备份，以便在不小心删除 IOS 文件或其他意外情况出现时，恢复路由器的 IOS 文件。一般使用 TFTP 的方式备份路由器的 IOS，本节的操作在真实的路由器上进行。本节以 Cisco 1841 路由器为例，使用如图 18-4-1 所示的连接方式，把计算机的网卡与路由器的 Fa0/0 口相连，直连或通过交换机中转均可；把路由器的 Console 端口通过配置线缆与计算机的 COM 口相连。

备份 IOS 文件的步骤如下：

① 安装 TFTP 服务器。在计算机上安装并运行 `tftpserver.exe`，把计算机配置成 TFTP 服务器。CCNANEW.rar 中包括了 `tftpserver.rar` 文件。

② 在路由器上 ping 192.168.1.200，测试路由器与计算机之间的连通性。

③ 检查计算机中 TFTP 服务器上的剩余空间，看是否足以保存 IOS 文件。IOS 文件一般都不超过 100MB，计算机硬盘一般都可以满足这个要求。

④ 查看 IOS 的文件名。使用命令如下：

```
R1#show flash
-#- --length-- -----date/time----- path
1      24355180 Feb 22 1907 17:31:44 +00:00 c1841-adviservicesk9-mz.124-9.t1.bin

7577600 bytes available (24358912 bytes used)
```

⑤ 开始备份。执行如下（斜体部分是注释）：

```
R1#copy flash tftp                                     把 Flash 拷贝到 TFTP 服务器上。
Source filename []?c1841-adviservicesk9-mz.124-9.t1.bin  IOS 文件的名字。
Address or name of remote host []? 192.168.1.200        TFTP 服务器的 IP 地址。
Destination filename [c1841-adviservicesk9-mz.124-9.t1.bin]?
拷贝到 TFTP 服务器上的名字，默认与 Flash 中的 IOS 文件名相同，直接回车就可以开始拷贝了，下面是拷贝的过程。
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
24358912 bytes copied in 146.552 secs (166214 bytes/sec)
```

拷贝完成后，可以在计算机的 TFTP 目录中找到 `c1841-adviservicesk9-mz.124-9.t1.bin` 文件。

2. 升级 IOS 文件

为了修复已知安全漏洞，支持新的高级特性，提高路由器的性能，有时需要升级 IOS。升级 IOS 前，先使用“show flash”命令检查 Flash 空间是否足以容纳新的 IOS，如果 Flash

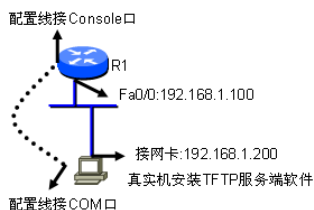


图 18-4-1 路由器文件管理

空间不足，则不要盲目升级。升级 IOS 的步骤如下：

```

R1#copy tftp flash      把 TFTP 服务器上的 IOS 文件拷贝到 Flash。
Address or name of remote host []? 192.168.1.200      TFTP 服务器的 IP 地址。
Source filename []? c1841-advispervicesk9-mz.124-9.t2.bin
要拷贝的 IOS 文件名字，在 TFTP 服务器中把刚才拷贝到的 IOS 文件随便改个名字。
Destination filename [c1841-advispervicesk9-mz.124-9.t2.bin]?
拷贝到 Flash 中的文件名，默认相同，这里直接回车。
Accessing tftp://192.168.1.200/c1841-advispervicesk9-mz.124-9.t2.bin...

Erase flash: before copying? [confirm]
路由器拷贝新的 IOS 前，询问是否删除老的 IOS 文件，一般 Flash 的空间有限，这里确认删除；如果 Flash
的空间很大，这里可按任意键，放弃删除。Flash 中如果有多个 IOS 文件，默认加载的是第一个 IOS 文件，或
者通过使用“boot system”命令修改，这一般在测试 IOS 的情况下使用。这里直接回车。
Erasing the flash filesystem will remove all files! Continue? [confirm]
再次进行确认。

Erasing device ...eeeeee 省略部分，erased      删除的过程，这里省略了部分输出。
Erase of flash: complete      删除完成。
Loading c1841-advispervicesk9-mz.124-9.t2.bin from 192.168.1.200 (via FastEthernet
0/0):
!!!!!! 省略部分!!!!!!
路由器开始拷贝新的 IOS 文件，此时一定不要断电，否则路由器将丢失 IOS。如果万一断电，可以使用接下来要
介绍的方法恢复 IOS 文件。拷贝完成后，重启路由器就可以了。

```

3. 恢复 IOS 文件

如果 IOS 文件不小心被删除或某些意外情况发生，造成路由器中 IOS 文件丢失，路由器不能正常启动，此时就需要恢复路由器的 IOS 文件。在路由器丢失 IOS 文件，不能正常启动的情况下，有两种恢复路由器 IOS 文件的方式：TFTP 和 Xmodem。TFTP 是推荐的使用方式，TFTP 方式使用路由器的带内（In-Band，就是使用网络传输）传输，速率非常快，一般不超过半小时就可以完成。有些型号的路由器可能不支持 TFTP 方式，就需要使用带外方式（Out-of-Band，不使用网络传输，也就是使用配置线缆传输），借助于 Xmodem 传输来恢复路由器 IOS，因为配置线缆的速率是 9600b/s，往往要花费几个小时的时间来传输路由器的 IOS 文件。

（1）TFTP 方式

- ① 首先保证图 18-4-1 连线正确，网线要连在路由器编号最小的以太网接口上。
- ② 删除路由器的 IOS 文件之前，一定要使用上面介绍的方法对 IOS 文件进行备份。删除路由器的 IOS 文件的命令如下（斜体部分是注释）：

```

Router#dir      查看路由器的 IOS 文件。
Directory of flash:/

 1  -rw-   24355180  Feb 22 1907 17:31:44 +00:00  c1841-advispervicesk9-mz.124-9.t1.bin

31936512 bytes total (7577600 bytes free)
Router#delete flash:c1841-advispervicesk9-mz.124-9.t1.bin      删除路由器的 IOS 文件。
Delete filename [c1841-advispervicesk9-mz.124-9.t1.bin]?      确认删除的文件名。
Delete flash:c1841-advispervicesk9-mz.124-9.t1.bin? [confirm] 确认删除。
Router#dir      再次查看路由器的 IOS，发现删除成功。
Directory of flash:/

No files in directory

31936512 bytes total (31936512 bytes free)
Router#

```

- ③ 使用 reload 命令重启路由器。

```
Router#reload
Proceed with reload? [confirm]
```

④ 路由器重新启动，因为找不到 IOS 文件，路由器进入 ROM monitor 模式，完整配置下列信息：

```
rommon 1 > IP ADDRESS=192.168.1.100
rommon 2 > IP_SUBNET_MASK=255.255.255.0
rommon 3 > DEFAULT_GATEWAY=192.168.1.1
rommon 4 > TFTP_SERVER=192.168.1.200
rommon 5 > TFTP_FILE=c1841-advipservicesk9-mz.124-9.t1.bin
```

接下来，对上述各行进行解释。

- rommon 1 > IP_ADDRESS=192.168.1.100，配置路由器的 IP 地址，这里要注意几行中的变量名称是区分大小写的，“=”号的前后不要包含任何空格，不要使用全角符号，高级的编辑功能也没有启用，变量名称输错也没有提示。如果可能，最好使用文本编辑器剪切和粘贴这些参数到终端窗口。
- rommon 2 > IP_SUBNET_MASK=255.255.255.0，配置子网掩码。
- rommon 3 > DEFAULT_GATEWAY=192.168.1.1，配置网关，也就是说，这种方式支持跨网段操作，如果 TFTP 服务器和路由器在同一个子网中，网关可以不配置。
- rommon 4 > TFTP_SERVER=192.168.1.200，TFTP 服务器的 IP 地址。
- rommon 5 > TFTP_FILE=c1841-advipservicesk9-mz.124-9.t1.bin，TFTP 服务器上 IOS 的文件名，文件名区分大小写。

⑤ 参数配置完成后，使用 tftpdnld 从 TFTP 服务器加载路由器的 IOS 文件，操作如下（斜体部分是注释）：

```
rommon 6 > tftpdnld
```

这个命令是 TFTP download 的意思，也就是通过 TFTP 下载，回车后，下面显示的是一些参数信息。

```

IP ADDRESS: 192.168.1.100
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 192.168.1.1
TFTP_SERVER: 192.168.1.200
TFTP_FILE: c1841-advipservicesk9-mz.124-9.t1.bin
TFTP_MACADDR: 00:15:2b:ee:f6:36
TFTP_VERBOSE: Progress
TFTP_RETRY_COUNT: 18
TFTP_TIMEOUT: 7200
TFTP_CHECKSUM: Yes
FE PORT: 0
FE SPEED MODE: Auto Detect

Invoke this command for disaster recovery only. 提醒信息，只在灾难恢复的时候才使用这个命令。
WARNING: all existing data in all partitions on flash will be lost!
警告信息：所有 Flash 中存放的文件都将被删除！
Do you wish to continue? y/n: [n]: y          要继续吗？回答 yes，继续。
.....
Receiving c1841-advipservicesk9-mz.124-9.t1.bin from 192.168.1.200 !!!!!!!!!!!!!!!
!!!!!!!!!!!!
省略部分路由器从 TFTP 服务器开始下载 IOS 文件。大约几分钟后，出现下面的提示：
File reception completed.          文件拷贝成功。
Validating checksum.               检验和检查。
Copying file c1841-advipservicesk9-mz.124-9.t1.bin to flash.
把文件拷贝到 Flash 中，刚才拷贝的内容只是放在内存中，检验无误后，才拷贝到 Flash 中。
省略部分
Initializing ATA monitor library.....
```

⑥ 重启路由器。

```
rommon 7 > reset
```

重新启动路由器。

路由器启动成功后,再次使用 `dir` 命令进行查看,可以发现 IOS 已经被恢复到 Flash 中。至此,完成了使用 TFTP 方式恢复路由器中的 IOS 操作。

(2) Xmodem 方式

① 在 ROM monitor 模式下输入 “`xmodem -c c1841-adviservicesk9-mz.124-9.t1.bin`” 命令,如图 18-4-2 所示,路由器提醒这种方式只在灾难恢复的情况下使用,是否要继续,输入 “y”,继续,屏幕显示 “Ready to receive file c1841-adviservicesk9-mz.124-9.t1.bin”。

② 单击超级终端的“传送”菜单→“发送文件”,打开“发送文件”对话框,如图 18-4-2 所示,在“文件名”栏中浏览到 IOS 文件所在的位置,在“协议”中选择“Xmodem”,单击“发送”按钮。

③ 接下来开始发送文件,文件发送成功后,使用 `reset` 命令重启路由器,恢复 Flash 中的 IOS 文件,这种恢复方式较慢,一般需要几个小时才能完成,在 TFTP 可用的情况下,不要使用 Xmodem 方式。

本节除 Xmodem 方式外的所有实验都可以在 Packet Tracer 模拟器中完成,使用 Packet Tracer 的实验拓扑如图 18-4-3 所示,读者可以在 Packet Tracer 模拟器中打开光盘中的“配置\18路由器文件管理.pkt”文件。

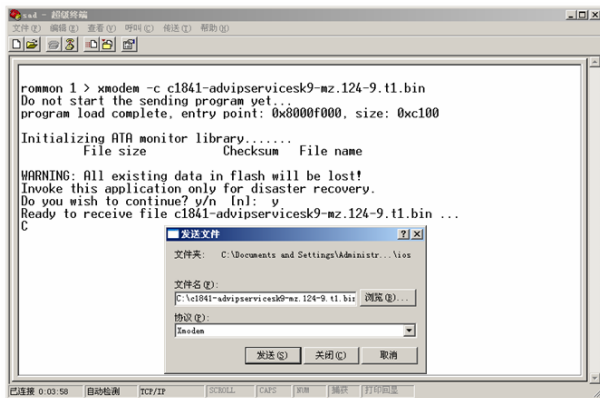


图 18-4-2 使用 Xmodem 方式恢复 IOS

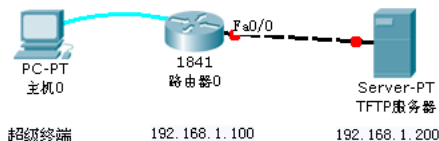


图 18-4-3 在 Packet Tracer 模拟器中管理 IOS

18.4.2 配置文件管理*

1. 备份配置文件

出于安全方面的考虑,可以对路由器的配置文件 (`startup-config`) 进行备份,以便在不小心删除配置文件或其他意外情况出现时,恢复路由器的配置文件。一般使用 TFTP 的方式备份路由器的配置文件,这里的实验可以在 CCNA 模拟机架中完成。

① 在真实机上安装并运行 TFTP 服务器端软件。

② 启动 CCNA 机架中的路由器 R1,并对路由器 R1 进行配置, Fa0/0 端口的 IP 地址是 192.168.1.100。

③ 测试路由器 R1 与真实机间的网络连通性。

```
R1#ping 192.168.1.200
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.1.200, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/16 ms
```

④ 开始备份。执行如下（斜体部分是注释）：

```
R1#wr                                保存配置。
Building configuration...
[OK]
R1#copy startup-config tftp          把启动配置文件拷贝到 TFTP 服务器。
Address or name of remote host []? 192.168.1.200  TFTP 服务的 IP 地址。
Destination filename [r1-config]?      拷贝到 TFTP 服务器上的文件名。
!!
865 bytes copied in 0.068 secs (12721 bytes/sec) 拷贝完成。
R1#
```

拷贝完成后，可以在计算机的 TFTP 目录中找到 r1-config 文件。

2. 恢复配置文件

命令如下：

```
R1#copy tftp startup-config
Address or name of remote host []? 192.168.1.200
Source filename []? r1-config
Destination filename [startup-config]?
Accessing tftp://192.168.1.200/r1-config...
Loading r1-config from 192.168.1.200 (via FastEthernet0/0): !
[OK - 865 bytes]
[OK]
865 bytes copied in 9.160 secs (94 bytes/sec)
R1#
```



18.5 密码恢复技术 ***

为了保证路由器和交换机的安全，需要采用密码技术。可是由于种种原因，比如忘记密码，或者由于人员的变动，没有做好工作交接，这时都需要使用密码恢复技术来恢复路由器和交换机的密码。CCNA 考试中特别注重路由器密码恢复技术或恢复中可能出现的问题，对交换机的密码恢复技术则很少涉及。

18.5.1 路由器密码恢复***

在 Packet Tracer 模拟器中打开光盘中的“配置\18\路由器密码恢复.pkt”文件，进入 PC 的“Desktop”标签，打开“Terminal”应用程序，进入路由器的用户配置模式，输入 enable，打算进入路由器的特权配置模式，提示输入特权密码，因为不知道特权密码，无法进入路由器的特权模式。接下来介绍路由器的密码恢复技术，密码恢复完成后，不允许丢失路由器原有的配置。操作步骤如下：

① 使用超级终端连接到路由器控制台端口。

② 如果忘记了特权密码，但仍可进入用户模式。可以使用“show version”命令查看路由器的配置寄存器值（斜体部分是注释）。该步骤对密码恢复一般没有什么用。

```
R1>show version          在用户模式下查看配置寄存器的值。
省略部分输出。
Configuration register is 0x2102
可以看到配置寄存器的值是 0x2102，一般路由器配置寄存器的值是 0x2102，这个值的意思是路由器启动时，
加载用户的配置文件，也就是加载 startup-config 文件。
```


该步骤对密码恢复一般没有什么用。除非配置寄存器的值是 0x2142，表示启动时不加载用户配置文件，但一般路由器都不会是这个值。

③ 使用电源开关关闭路由器 R1，然后再给路由器 R1 加电重启。

④ 在路由器重新启动的 60 秒内，按计算机键盘上的“Ctrl + Break”组合键，稍后路由器进入 ROMmon 模式，如图 18-5-1 所示。

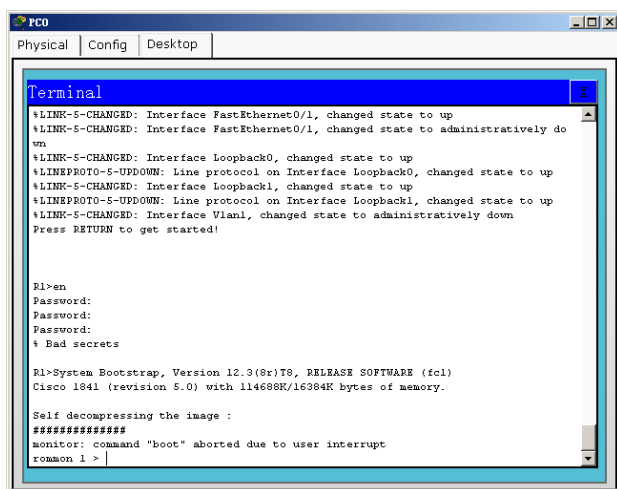


图 18-5-1 恢复路由器密码

⑤ 修改配置寄存器的值为 0x2142，使路由器启动时跳过配置文件。配置如下：

```
rommon 1 > confreg 0x2142
```

修改配置寄存器的值为 0x2142，注意前面的是数字“0”，不是字母“o”。有些型号的路由器上输入的是 o/r 0x2142，注意“o/r”中的是字母“o”，不是数字“0”。You must reset or power cycle for new config to take effect
真实路由器会出现这句提示，模拟器上没有出现。提示需要输入 reset 或断电重启。

⑥ 重启路由器。

```
rommon 2 > reset
```

重启路由器并忽略保存的配置。

⑦ 路由器重新启动，提示“Would you like to enter the initial configuration dialog? [yes/no]:”，感觉像一台新的路由器一样，其实路由器是有配置文件的，只是没有被加载而已，回答“no”。输入 enable，路由器没有提示输入密码，就进入特权模式。

⑧ 把 NVRAM 中的配置文件拷贝到内存中。

```
Router#copy startup-config running-config
```

注意：这一步一定要做，如果不拷贝，而是直接修改密码并保存，老的启动配置文件将被覆盖，新保存的配置文件中仅有路由器的默认配置和密码，以前的有用配置都丢失了。

⑨ 使用“show running-config”命令，会看到一些密码，比如：enable password、enable secret、vty、console 密码等，如果密码被加密了，重新输入新的密码。

```
Router(config)#enable pass cisco
Router(config)#enable secret cisco!##%
Router(config)#line vty 0 4
Router(config-line)#password cisco@#$%
Router(config-line)#line console 0
Router(config-line)#password cisco#$%^
```

⑩ 使用“no shutdown”命令，打开所有使用的端口。因为“copy startup-config running-config”是把 startup-config 和 running-config 作了一个简单的合并，很多过去使用的端口在 running-config 中的配置是 shutdown，在合并后的最终 running-config 文件中，这些端口仍然被关闭，所以需要把一些使用的端口手工打开。

⑪ 改回配置寄存器的值，命令如下：

```
R1(config)#config-register 0x2102
```

要记得把配置寄存器的值改回 0x2102，不然，以后路由器重启后，仍然不加载用户的配置文件，影响使用。

⑫ 保存配置。使用“write”或“copy running-config startup-config”命令，保存路由器的配置。至此，路由器的密码恢复成功。

18.5.2 交换机密码恢复*

路由器的密码恢复比较常见，主要是通过修改配置寄存器的值来实现。在实际使用过程中，不仅要接触路由器设备，交换机也经常被使用到。下面介绍交换机的密码恢复技术，思科的 2900 系列和 3500 系列交换机的密码恢复技术相同，Packet Tracer 模拟器中的交换机没有提供 MODE 按键，不支持密码恢复操作。接下来的操作是在真实的思科交换机上完成的。

① 用 Console 线连接交换机的 Console 端口和计算机的 COM 口。使用超级终端连接到交换机。

② 断电重新启动交换机，并且在启动过程中按下交换机前面板上的 MODE 按键，大概 10 秒钟左右，交换机上的屏幕显示如下：

```
The system has been interrupted prior to initializing the
flash filesystem. The following commands will initialize
the flash filesystem, and finish loading the operating
system software:
```

```
flash_init
load_helper
boot
```

```
switch:
```

③ 加载 flash_init，在 switch:提示符下输入“flash_init”，交换机执行如下：

```
switch: flash_init
Initializing Flash...
flashfs[0]: 11 files, 1 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 3612672
flashfs[0]: Bytes used: 1816064
flashfs[0]: Bytes available: 1796608
flashfs[0]: flashfs fsck took 4 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
switch:
```

④ 在 switch:提示符下输入“load_helper”后回车，启动交换机的管理助手。

```
switch: load_helper
```

⑤ 查看当前交换机的 Flash 信息，命令为“dir flash:”。可以看到当前交换机中的所有文件，有一个名为 config.text 的文件，这就是交换机启动时加载的配置文件。

```
switch: dir flash:
```

```
Directory of flash:/
```

```

2  -rw- 1797760  <date>          c3500x1-c3h2s-mz.120-5.WC5
3  -rw- 676      <date>          server
4  -rw- 616      <date>          vlan.dat
5  -rw- 3        <date>          env_vars
6  -rw- 1929     <date>          config.text

```

```
1796608 bytes available (1816064 bytes used)
```

⑥ 将文件重新命名。

```
switch: rename flash:config.text flash:config.old
```

使用“`rename flash:config.text flash:config.old`”命令把 `config.text` 修改为 `config.old` 后，就可以实现密码恢复工作了。因为原来的密码信息都保存在 `config.text` 文件中，当交换机启动时没有找到 `config.text` 文件就将无法加载初始密码信息，从而可以通过空密码来登录交换机进行管理操作。这里采用的原理和路由器的密码恢复原理相同。

⑦ 修改完成后，使用 `boot` 命令重新启动交换机，让 IOS 信息重新加载。

```
Switch:boot
```

⑧ 交换机重新启动后，出现“Continue with configuration dialog? [yes/no]:”信息，回答 `no`，进入交换机的用户配置模式，输入 `enable` 进入交换机的特权模式。将之前修改的 `config.old` 文件名还原成 `config.text`。命令如下：

```
Switch#rename flash:config.old flash:config.text
Destination filename [config.text]?
Switch#
```

⑨ 加载 `config.text` 文件中的信息，命令如下：

```
Switch#copy startup-config running-config
Destination filename [running-config]?
1929 bytes copied in 1.867 secs (1929 bytes/sec)
```

⑩ 查看 `running-config` 文件中的相关密码，包括 `enable password`、`enable secret`、`vtty`、`console` 密码等，如果密码被加密了，重新输入新的密码。

```

Switch (config)#enable pass cisco
Switch (config)#enable secret cisco!##%
Switch (config)#line vty 0 4
Switch (config-line)#password cisco@#$%
Switch (config-line)#line console 0
Switch (config-line)#password cisco#$%^

```

⑪ 保存配置。使用“`write`”或“`copy running-config startup-config`”命令，保存交换机的配置。至此，交换机的密码恢复成功。



18.6 真题精选***

1. Which type of attack is characterized by a flood of packets that are requesting a TCP connection to a server?

- A. denial of service
- B. brute force
- C. reconnaissance
- D. Trojan horse

2. What are two recommended ways of protecting network device configuration files from outside network security threats? (Choose two.)

- A. Allow unrestricted access to the console or VTY ports.
- B. Use a firewall to restrict access from the outside to the network devices.

- C. Always use Telnet to access the device command line because its data is automatically encrypted.
- D. Use SSH or another encrypted and authenticated transport to access device configurations.
- E. Prevent the loss of passwords by disabling password encryption.
- 3. What are two security appliances that can be installed in a network? (Choose two.)
 - A. ATM
 - B. IDS
 - C. IOS
 - D. IOX
 - E. IPS
 - F. SDM
- 4. What should be part of a comprehensive network security plan?
 - A. Allow users to develop their own approach to network security.
 - B. Physically secure network equipment from potential access by unauthorized individuals.
 - C. Encourage users to use personal information in their passwords to minimize the likelihood of passwords being forgotten.
 - D. Delay deployment of software patches and updates until their effect on end-user equipment is well known and widely reported.
 - E. Minimize network overhead by deactivating automatic antivirus client updates.
- 5. Refer to the exhibit. What is the effect of the configuration that is shown?

```
line vty 0 4
password 7 030752180500
login
transport input ssh
```

- A. It configures SSH globally for all logins.
- B. It tells the router or switch to try to establish an SSh connection first and if that fails to use Telnet.
- C. It configures the virtual terminal lines with the password 030752180500.
- D. It configures a Cisco network device to use the SSH protocol on incoming communications via the virtual terminal ports.
- E. It allows seven failed login attempts before the VTY lines are temporarily shutdown.
- 6. What are two characteristics of Telnet? (Choose two.)
 - A. It sends data in clear text format.
 - B. It is no longer supported on Cisco network devices.
 - C. It is more secure than SSH.
 - D. It requires an enterprise license in order to be implemented.
 - E. It requires that the destination device be configured to support Telnet connections.
- 7. Refer to the exhibit. Why is flash memory erased prior to upgrading the IOS image from the TFTP server?
 - A. The router cannot verify that the Cisco IOS image currently in flash is valid.
 - B. Flash memory on Cisco routers can contain only a single IOS image.
 - C. Erasing current flash content is requested during the copy dialog.
 - D. In order for the router to use the new image as the default, it must be the only IOS image in flash.

```

Router#copy tftp flash
Address or name of remote host []? 192.168.1.200
Source filename []? c1841-advipservicesk9-mz.124-9.t2.bin
Destination filename [c1841-advipservicesk9-mz.124-9.t2.bin]?
Accessing tftp://192.168.1.200/c1841-advipservicesk9-mz.124-9.t2.bin
Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing Device ...
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeee, erased
      Erase of flash: complete
      Loading c1841-advipservicesk9-mz.124-9.t2.bin from 192.168.1.200 (via FastEthernet 0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 6888962/13777920 bytes]

Verifying checksum... OK (0x7BF3)
6888962 bytes copied in 209.920 secs (32961 bytes/sec)
Router#

```

8. When upgrading the IOS image, the network administrator receives the exhibited error message. What could be the cause of this error?

```

Router1#copy tftp flash
Address or name of remote host[]? 192.168.1.5
Source filename[]? c2600-js-1-121-3.bin
Destination filename | c2600-js-1-121-3.bin
Accessing tftp://192.168.1.5 /c2600-js-1-121-3.bin...
%Error opening tftp://192.168.1.5 /ICCC (Timed out)

```

- A. The new IOS image is too large for the router flash memory.
- B. The TFTP server is unreachable from the router.
- C. The new IOS image is not correct for this router platform.
- D. The IOS image on the TFTP server is corrupt.
- E. There is not enough disk space on the TFTP server for the IOS image.



18.7 真题解答***

1. 解：A

题目问：哪种类型攻击的特征是泛洪包，请求服务器的 TCP 连接？可以参照本章 18.1.3 节，DoS（Denial of Service，拒绝服务）攻击者想办法让目标机器停止提供服务或资源访问，这些资源包括磁盘空间、内存、进程甚至网络带宽，从而阻止正常用户的访问。本题中讲到的 TCP 请求攻击是 DoS 攻击中的一种 SYN Flood（SYN 洪水）攻击。

2. 解：BD

哪两种是推荐的方法，用来保护网络设备配置文件不会受到网络外部的威胁？参照本章 18.2.2 节，要确保外部的安全站点才可以访问网络设备，可以使用防火墙来限制外网访问网络中的设备；使用 SSH 或其他加密和认证的传输来访问网络配置，比如管理员经常使用 Telnet 来远程管理网络设备，要知道 Telnet 是一个明文传输的协议（包括敏感的密码），很容易受到窃听，从而泄露机密。

3. 解: BE

题目问: 哪两个安全产品可以被安置在网络中(选两个)? 参照本章 18.1.4 节, IDS 和 IPS 是两个安全产品。ATM 是网络类型, IOS 是思科设备的网络操作系统, SDM 是设备管理软件, 都不是产品, 据目前所学, 并没有介绍过 IOX。

4. 解: B

题目问: 什么是广泛网络安全计划的一部分? 可以参照本章 18.1.4 节, A 选项说, 允许用户用自己的方法部署网络安全, 网络安全是一个整体规划, 该选项错; B 选项说, 物理上保护网络设备的安全, 阻止一些潜在的没有授权的个体访问, 该选项正确; C 选项说, 鼓励用户使用个人的信息当做密码, 从而减小密码被忘记的可能性, 该选项错, 个人信息很容易被猜测到; D 选项说, 延迟部署软件的补丁, 该选项错, 软件的补丁一定要及时更新; E 选项说, 为了减轻网络的负载, 不要激活防病毒软件的自动更新功能, 该选项错, 防病毒软件要实时更新, 才能有效防御病毒。

5. 解: D

参照图, 题目问: 图中显示配置的影响是什么? 可以参照本章 18.2.2 节, 这里配置的是使用 SSH 协议访问思科网络设备的 VTY 端口, 因为默认使用的 Telnet 协议是一个明文传输的协议, 容易泄露机密。

6. 解: AE

题目问: Telnet 的两个特点是什么(选两个)? 可以参照本章 18.2.2 节, 首先 Telnet 是一个明文传输协议; 其次要求目标设备被配置支持 Telnet 连接, 在默认情况下, 思科设备的 VTY 线路要求登录, 但并没有配置密码, 此时不允许 Telnet 会话, 要么是使用“no login”命令取消 VTY 要求登录的设置, 要么是在 VTY 线路上使用“password”命令配置密码, 来允许远程的 Telnet 连接。

7. 解: C

题目问: 参照图, 从 TFTP 服务器更新 IOS 文件前, 为什么删除 flash (闪存, 用于保存 IOS) 存储? 可以参照本章 18.4.1 节, 路由器拷贝新的 IOS 前, 询问是否删除老的 IOS 文件, 一般 Flash 的空间有限, 这里确认删除; 如果 Flash 的空间很大, 这里可按任意键, 放弃删除。Flash 中如果有多个 IOS 文件, 默认加载的是第一个 IOS 文件, 或者通过使用“boot system”命令修改。综上所述, 删除 Flash 存储是复制对话的要求, 在 Flash 空间大的情况下也可以不删除, C 选项正确; A 选项说无法验证路由器当前使用的 IOS 是否合法, 该说法错误, 如果 IOS 不合法, 路由器的当前操作也无法进行了; B 选项说 Flash 中只能包含一个 IOS 文件, 该说法错误, 只要 Flash 空间够大, 就可以包含多个; D 选项说路由器默认加载 Flash 中的第一个 IOS 文件, 升级的 IOS 文件必须是 Flash 中仅有的一个文件, 该说法错误, 可以使用“boot system”命令指定加载的 IOS 文件。

8. 解: B

题目问: 当更新 IOS 文件时, 网络管理员收到图中显示的错误信息, 是什么原因导致了错误? 可以参照本章 18.4.1 节, 这里提示的是打开 tftp://192.168.1.5/超时, 即访问 TFTP 服务器失败, 还没有涉及服务器上有没有这个 IOS 文件, 以及这个 IOS 文件的大小等问题。

第 19 章

远程办公*

本章主要描述企业提供远程办公服务的需求；介绍如何使用 DSL（Digital Subscriber Line，数字用户线路）、Cable 和无线技术扩展宽带服务；介绍 VPN（Virtual Private Networks，虚拟私有网络）技术、VPN 好处、VPN 的配置等，以期提供安全、快速和可靠的远程网络连接，为远程办公服务。

本章内容在 CCNA 考试中很少出现。



19.1 远程办公的商业需要

远程办公（Teleworker）是指远离办公场所，通常是从一个 SOHO（Small Office or Home Office，小型办公室或家庭办公室）借助通信支持连接到工作场所。

19.1.1 远程办公的优势

越来越多的公司发现了远程办公的优势。随着宽带和无线技术的发展，远程办公不再面临过去的挑战，人们可以远程办公，感觉就像在公司一样。企业可以高效地分发数据、语音、视频和实时应用程序，而不用考虑用户有多远以及有多分散。远程办公可以超越时间和空间的限制，为企业赚取更多的利润。

对日常业务来说，远程办公也是有益的。在糟糕的天气、交通拥塞、自然灾害或其他不可预测的情况下，远程办公使工作人员不用赶到办公场所，从而保证工作的连续性。在更广泛的规模下，企业可以借助远程办公提供跨越时区和国界的服务。现在很多跨国公司、国际集团都可以借助网络实现视频会议、远程办公和统一调度等。

从社会的角度来看，远程办公还可以增加就业机会，使一些处在偏远地区或行动不便的人也可获得就业机会。

19.1.2 远程办公的解决方案

远程办公网是企业用来连接 SOHO 用户、分支办公室、总部或合作单位的网络，不同于一般的远程连接，远程办公除了需要考虑费用外，更要考虑到安全和可靠。

这里介绍可以支持远程办公服务的3种远程连接技术：

- **传统广域网中专用的第 2 层技术。**包括帧中继（Frame Relay）、ATM 和租用线路，提供了很多的远程连接解决方案。这些连接的安全性依赖于服务提供商。
- **远程（VPN）。**一般是 SOHO 用户或移动用户通过宽带（包括 Cable 或 DSL）或无线接入互联网，通过在个人电脑上安装 VPN 客户端软件，来连接到远程办公场所。

提供灵活和可扩展的连接。

- **站点到站点 VPN**。一般用于不同的站点之间，比如总部、分支机构和合作单位之间。一般需要 VPN 路由器、VPN 集中器或多功能的安全设备等硬件来实现连接，可以为远程办公提供一个安全、快速和可靠的远程连接，这是远程办公最常见的连接方式。

远程办公用户通过加密的 VPN 隧道连接到公司网络，这是安全和可靠的连接。VPN 是利用公共电信基础设施传输私有数据的网络，VPN 使用隧道协议和安全程序保护隐私。

本章介绍的 IPSec (IP 安全) 协议作为建立安全 VPN 隧道最受欢迎的方法，工作在网络层。



19.2 宽带服务*

远程办公通常使用的不同应用（例如，电子邮件、关键应用、实时协作、语音、视频等）需要一个高带宽连接。当连接远程办公时，第一考虑的就是选择接入网络的技术以确保有合适的带宽。

Cable、DSL 和无线宽带可以满足远程办公用户带宽的需要。调制解调器建立的拨号连接虽然为移动访问或旅行时提供了便利，但慢速的带宽通常满足不了远程办公的需要。只有在其他选项不可以使用的情况下，才考虑使用调制解调器建立拨号连接来为远程办公服务。

远程办公用户需要先连接到一个 ISP (Internet 服务供应商) 来访问 Internet。ISP 提供了不同的连接选项用来连接家庭和小型企业用户，它们的连接拓扑如图 19-2-1 所示。

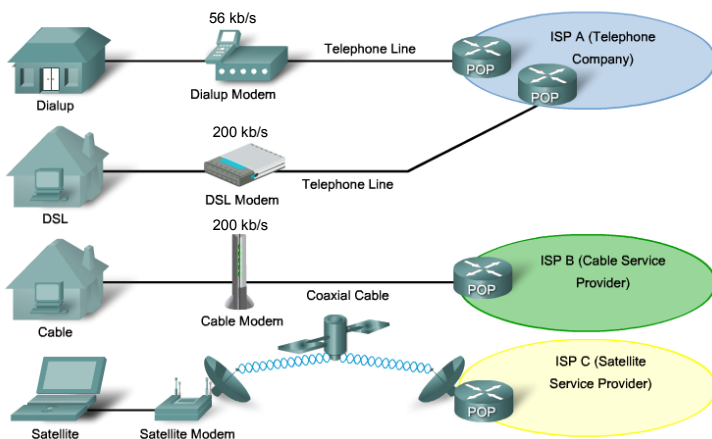


图 19-2-1 SOHO 用户连接拓扑

- **拨号上网**。一种廉价的选择，使用任何电话线和调制解调器。用户呼叫 ISP 的接入电话号码，连接到 ISP。拨号上网是最慢的连接选项，通常用于移动工作的地方，不适合对带宽高需求的应用。连接速度一般在 56kb/s 左右。
- **DSL**。通常比拨号上网昂贵，但提供了一种更快速的连接。DSL 也使用电话线，但和拨号不同，DSL 提供连续的连线服务。DSL 使用一种特殊的超高速调制解调器从电话信号中分出 DSL 信号，并提供一个以太网连接到一个主机电脑或网络。连接速度可以达到 200kb/s 或更高。
- **Cable Modem (电缆调制解调器)**。由有线电视服务供应商提供。互联网信号和有线

电视信号同在同轴电缆上转输。一个特殊的电缆调制解调器把互联网信号从同轴电缆上传输的其他信号中分离出来，并提供一个以太网连接到一个主机或网络。连接速度可以达到 200kb/s 或更高。

- 卫星。由卫星服务供应商提供。计算机通过以太网连接到一个卫星调制解调器，传输无线电信号到最近的卫星网络 POP（Point Of Presence）。连接速度从 128kb/s～512kb/s。

1. Cable Modem（电缆调制解调器）

远程办公通过有线电视网络访问互联网，再连接到企业的网络。同轴电缆是主要媒介，用来建立有线电视系统。

Cable 连接主要是硬件方面的知识，CCNA 考试中几乎不涉及这一部分知识，本书对此不做介绍。

2. DSL（数字用户线路）

DSL 是在已安装的铜线上提供高速连接的一种手段。铜质的电话线可以提供高达 1MHz 的频宽，而 POTS（Plain Old Telephone Service，老式电话服务）使用的频宽一般是 0～4kHz。DSL 对现有电话基础设施进行相对较小的改变，来为用户提供高带宽的数据传输速率。DSL 在用户和中心局（CO）之间建立连接，使用较高的传输频率（20kHz～1MHz），在有限距离内可以在传统铜线上实现较高带宽的传输（最快可达到 52Mb/s）。DSL 的特点如下：

- 能同时实现下载和上传。
- 可提供对称和非对称服务。所谓的非对称是指上传和下载的速率不同，常见的 ADSL（Asymmetric DSL，非对称 DSL）就采用了非对称的技术，下载最快可以达到 8Mb/s，上传最快可以达到 1Mb/s。
- 多种 DSL 技术，如表 19-2-1 所示。
- 语音和数据可以同时传输。有些 DSL 技术支持数据和语音同时传输，也就是数据传输和语音通话可以同时进行，在中国使用比较普遍的 ADSL 就支持语音和数据同时传输。
- 总是在线的数据连接。DSL 是纯数字的线路，连接始终建立，不像拨号上网，需要选择呼叫才能建立连接。
- 带宽与距离成反比。传输的距离越远，带宽越小。

表 19-2-1 各种DSL技术

DSL 技术	特 点	最大速度（下载/上传）b/s	是否支持数据和语音同时传输
ADSL	非对称	8M / 1M	是
VDSL	对称/非对称	52M / 13M	是
IDSL	对称	144k / 144k	否
SDSL	对称	768k / 768k	否
HDSL	对称	2M / 2M	否
G.SHDSL	对称	2.3M / 2.3M	否

CCNA 考试中几乎不涉及 DSL 连接的硬件知识，本书对此不做介绍。

3. Broadband Wireless（无线宽带）

有关无线的知识，本书第 13 章已经介绍过了。



19.3 VPN **

互联网是一个世界性的网络，由于其全球性，它已成为一种受欢迎的互联远程站点的方式。然而，Internet 是一个公共的网络，企业通过 Internet 来连接远程站点和传输数据，容易对企业内部网络构成安全威胁。幸运的是，VPN 技术能够让企业在互联网的基础上创建私有网络来提供机密性和安全性。

虚拟专用网（VPN）被定义为通过一个公用网络（通常是 Internet）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网是对企业内部网的扩展。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。虚拟专用网可用于不断增长的移动用户的全球 Internet 接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路，用于经济有效地连接到商业伙伴和用户的安全虚拟专用网。

19.3.1 VPN 优点**

VPN 可以给企业带来更大的灵活性和更高的生产力，几乎可以从任何地方的远程站点和远程办公室安全地连接到企业网络。VPN 对数据加密阻止非法用户破译。VPN 也允许远程主机访问防火墙的内部，远程用户就像在公司内一样使用网络设备。VPN 的优点如下：

- **Cost savings**（节省费用）。如果企业放弃租用专线或电话拨号方式而采用 VPN 联网来存取公司的数据，可以大大降低企业成本。
- **Scalability**（可扩展性）。能够随着网络的扩张，很灵活地加以扩展。当增加新的用户或子网时，只需修改已有的网络软件配置，在新增客户机或网关上安装相应软件并接入 Internet 后，新的 VPN 即可工作。
- **Security**（安全性）。高级的加密和验证协议阻止未授权的访问。

19.3.2 VPN 类型**

基于 IPSec VPN 的网络大致上可以分为两大类：站点到站点 VPN 和远程访问 VPN。

1. 站点到站点 VPN

在一个站点到站点的 VPN 中，主机通过 VPN 网关发送和接收 TCP/IP 流量，VPN 网关可以是一台路由器、PIX 防火墙或者 ASA（Adaptive Security Appliances，自适应安全设备）。VPN 网关负责封装和加密数据，并通过 VPN 隧道发送。在接收端，VPN 网关剥去头部，解密内容后，再将数据包发送到内网中的目标主机。

站点到站点 VPN 面向的对象是端对端网络，例如：公司总部与分支办公室的连接，这种连接以往都是通过专线或帧中继来完成的。站点到站点 VPN 与传统的专线连接相比，具有很大的价格优势。如图 19-3-1 所示就是一个使用 VPN 进行站点到站点连接的拓扑图。

2. 远程访问 VPN

远程访问 VPN 技术是拨号网络技术的革新，它是为移动办公用户提供服务的。多数远程用户可以从家中访问 Internet，使用宽带连接建立远程 VPN。同样，移动办公用户也可以使用本地电话与当地的 ISP 联系，以通过 ISP 访问国际互联网，进而建立 VPN 的连接。如图 19-3-2 所示，移动用户或家庭用户以及远程办公室先通过本地的 ISP 接入 Internet，然后

再通过 Internet 安全地接入公司网络中。在远程访问 VPN 中，每个主机一般都有 VPN 客户端软件。当主机发送数据之前，VPN 客户端软件对数据进行封装和加密。在接收端，VPN 网关处理数据的方式与站点到站点 VPN 中的处理方式相同。

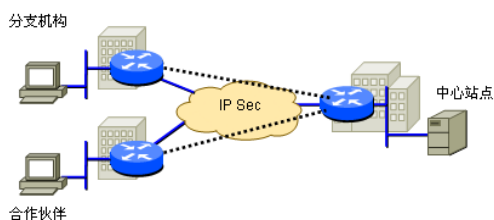


图 19-3-1 站点到站点 VPN

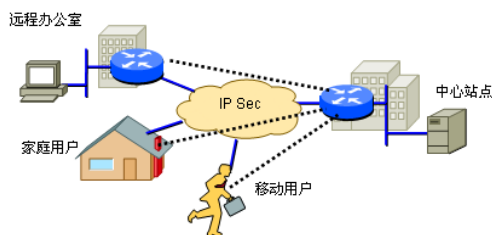


图 19-3-2 远程访问 VPN

19.3.3 VPN 安全性***

VPN 使用高级加密和隧道技术来允许企业在 Internet 上建立安全的、端到端的私有网络，VPN 提供的保护功能有：数据机密性、数据完整性和认证等。

1. 数据机密性（Data confidentiality）

数据机密性的定义是：数据发送方使用数学方法对数据进行加密，使数据在传输过程中变得不可读；数据接收方对接收到的数据使用一定的算法对其进行解密，最后将数据还原成原来的样子。在数据传输的过程中，即使被非法用户截获，可是因为传输的数据被加密，非法用户不知道密钥，得不到被加密前的真实数据。比如您给女朋友发信，里面有一些很肉麻的话，您不希望别人看到信的真实内容，那么您就可以使用加密。

（1）加密算法

加密算法大致上可以分为两类：对称式加密和非对称式加密。对称式加密是指发送方和接收方使用相同的密钥来加密和解密数据；非对称式加密是指发送方和接收方使用不同的密钥来加密和解密数据。

对称式加密算法有：DES、3DES、AES。其中，DES 使用 56 位密钥进行加密；3DES 是 DES 算法的变种，它使用 3 个独立的 56 位密钥对数据进行加密，解密，再加密的处理，安全性比 DES 强，当然占用处理器的时间也比 DES 长；AES 是后来的加密标准，用来取代 DES 加密技术，它比 DES 更安全，比 3DES 更高效。从加密的强壮程度上讲，3DES 优于 DES，AES 优于 3DES。AES 提供了 3 种不同长度的密钥：128 位、192 位和 256 位，就目前来说，128 位的密钥可以被认为是安全的，192 位和 256 位则提供了更高的安全性。

图 19-3-3 描述了对称式加密和解密的过程，发送方使用密钥加密，接收方使用同样的密码进行解密。因为加密和解密使用的密钥相同，所以要保证密钥的安全，如果密钥泄露出去，加密就失去意义了。对称式加密一般用于对数据内容的加密。

非对称式加密算法有：RSA。图 19-3-4 描述了非对称式加密的过程，发送方和接收方各生成两个密钥：私钥和公钥，并且将公钥发送给对方（私钥自己保留）。发送方在发送数据时使用接收方的公钥进行加密，接收方使用自己的私钥进行解密。由于公钥和私钥成对出现，只有使用对应的私钥才能解密公钥对数据的加密，因此整个通信过程是安全的。因为公钥是要发布出去的，所有人都可能获得，为了保证不能从公钥破解出私钥，这就要求公钥要有一定的长度来保证复杂性，RSA 的密钥长度为 512 位、768 位、1024 位或者更

长。因为 RSA 密钥很长，所以 RSA 算法的运行效率不高。IPSec 不使用 RSA 对数据内容加密，因为数据内容太多，执行效率太低，一般使用 RSA 进行数字签名和密钥本身的交换，这样加密的信息量不大。

(2) DH 密钥交换

无论是 DES、3DES、AES 还是 RSA，它们都需要使用密钥，这就引出一个问题：IPSec 对等体如何生成密钥呢？

DH (Diffie-Hellman, 发明此算法的两个人的名字) 密钥交换可以为对等体生成加密所需的密钥，它的算法也因强壮程度不同而分为 DH 组 1、DH 组 2、DH 组 5 和 DH 组 7。图 19-3-5 描述了 DH 的简要过程。

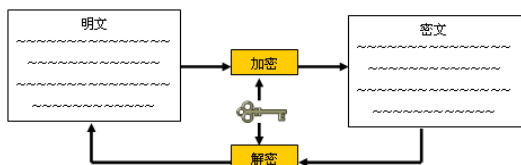


图 19-3-3 对称式加密算法

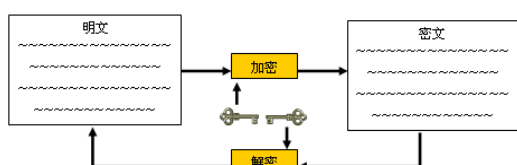


图 19-3-4 非对称式加密算法

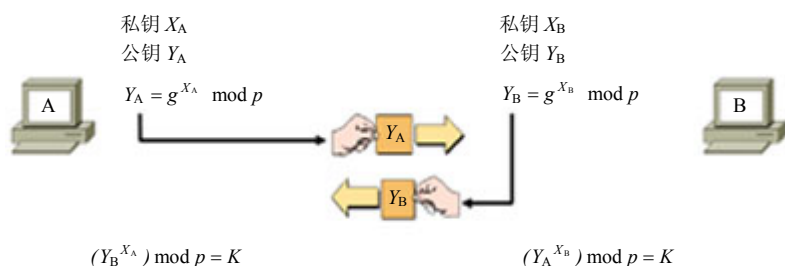


图 19-3-5 DH 过程

DH 算法比较复杂，除非进行理论研究，读者没必要了解详细过程。大概的过程是用户 A 和 B 产生各自的私钥和公钥，并且互相交换公钥，然后用自己的私钥和对方的公钥进行计算，最终算出相同的共享密钥，再使用相同的共享密钥对数据进行加密。为了保证共享密钥不会被破解，还可以设置共享密钥的生存周期，链路重新建立或密钥生存周期到达时，两端的 DH 算法重新计算，产生另一个相同的共享密钥，然后用此新产生的共享密钥对数据进行加密。

2. 数据完整性 (Data integrity)

数据完整性用于保证数据在传输过程中不被修改。如图 19-3-6 所示，发送方在发送数据时，为消息附加了一个 Hash 值 1。该 Hash 值 1 是消息源文和共享密钥经过 Hash 算法（也称散列算法）得出的一个值，Hash 算法本身的不可逆性保证了中间接收者很难根据 Hash 值 1 算出共享密钥。接收方在接收数据时，根据消息内容和共享密钥计算出 Hash 值 2，如果计算出的 Hash 值 2 和消息中附加的 Hash 值 1 一样，则说明数据没有被篡改。要知道数据的完整性并不提供数据的机密性，完整性仅仅保证数据在传输过程中没有被篡改。比如您要发一份信给女朋友，可担心中间有人篡改了信的内容，这时就可以使用数据的完整性，当女朋友收到信件时可以发现信的内容有没有被篡改过。

Hash 算法使用共享密钥将不同长度的消息转换成固定长度的字符串，有助于数据的完

完整性检查和验证, 确保传送的信息没有被篡改。一个哈希值 (Hash 值), 也称为消息摘要, 是从文本字符串算出的一串字符。哈希值远小于文本本身。它是利用一个公式, 在这个公式下, 不同的文字几乎不会产生相同的哈希值。其运算过程是不可逆的, 也就是说, Hash 值是无法被还原成消息的。Hash 值是附加在消息中发送的, 如果消息在传输过程中被修改, 接收方重新计算的 Hash 值和消息中原本附加的 Hash 值就无法匹配。

目前有两种常用的散列算法: HMAC-MD5 和 HMAC-SHA-1。其中 HMAC-MD5 是不定长度的文本和 128 位的共享密钥经过运算, 产生一个 128 位的 Hash 值, Hash 值和文本一起被发送到远端。而 HMAC-SHA-1 使用的是 160 位共享密钥进行散列计算, HMAC-SHA-1 更安全, 但占用的资源相对也多。

! 注意: 单纯使用数据完整性检查只能识别数据有没有被篡改, 并不能保证数据不泄密, 在图 19-3-6 中可以看到, 发送的数据仍然是明文。

3. 认证 (Authentication)

认证有时也叫起源认证, 即对对等体进行验证, 也称对等体验证 (Peer Authentication), 是指对数据发送者的身份进行识别, 确保信息的来源真实可信。起源认证可以使用密码、数字证书、智能卡和生物特征对数据来源进行认证。这里还以发信为例, 前面介绍过可以通过数据的机密性来保证信的内容不被非法读取, 使用数据的完整性来保证信的发送过程中没有被篡改。可是如果别人以您的名义、您的信箱给您的女朋友发信, 结果会如何呢? 所以, 除了数据的机密性和完整性外, 还需要对数据的起源进行认证, 比如您的女朋友收到信件后能对信件的来源进行认证, 识别出冒充的信件。

起源认证目前主要有两种方法: 预共享密钥、RSA 签名。

(1) 预共享密钥 (Pre-Shared Key, PSK)

预共享密钥是指在 IPsec 对等体上预先设置好相同的密钥, 当它们进行认证时, 发送方将预共享密钥和身份信息进行散列计算, 然后将计算出的散列发送给接收方; 接收方对收到的消息进行散列处理, 如果能生成相同的散列, 则发送方被验证。预共享密钥比较容易配置, 但是扩展性很不好, 仅使用于小型 VPN 网络中。如图 19-3-7 所示, 与图 19-3-6 相似, 只不过图 19-3-6 中是文本信息和共享密钥经过 Hash 算法, 来保证文本信息的完整性, 这里是身份信息和共享密钥经过 Hash 算法, 来保证身份信息的完整性, 即身份是真实可信的, 没有被修改过。

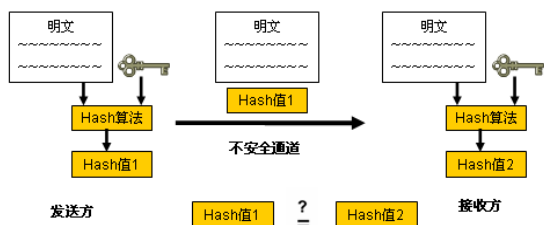


图 19-3-6 数据完整性检查

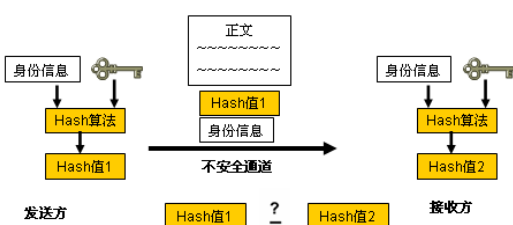


图 19-3-7 预共享密钥验证起源

(2) RSA 签名

RSA 签名的过程和 RSA 数据加密的过程恰好相反。发送方使用自己的私钥对身份信息进行加密, 形成签名, 接收方使用发送方的公钥对签名进行解密, 将解密得到的身份信息

与发送过来的明文身份信息进行比较, 如果一致, 则签名被确认。



注意: 单纯使用起源认证只能识别数据的起源, 并不能保证数据不泄密和没有被修改。

19.3.4 IPSec 安全协议**

通信双方如果要用 IPSec 建立一条安全的传输通路, 需要事先协商好将要采用的安全策略, 包括使用的加密算法、密钥、密钥的生存期等。当双方协商好使用的安全策略后, 就说双方建立了一个安全关联。安全关联就是能向其上的数据传输提供某种 IPSec 安全保障的一个简单连接, 可以由 AH 或 ESP 提供。

1. ESP (Encapsulating Security Payload, 封装安全负载)

ESP 主要用来对有效负荷进行保护, 此外对数据完整性认证、起源认证和防重放保护也提供某种程度的支持。ESP 是与具体的加密算法相独立的, 几乎可以支持各种对称密钥加密算法, 例如 DES、3DES、AES 等。使用 ESP 进行安全通信之前, 通信双方需要先协商好一组将要采用的加密策略, 包括使用的算法、密钥以及密钥的有效期等。

2. AH (Authentication Header, 验证头部)

AH 可以确保数据完整性、提供起源认证和防重放保护, 但是 AH 不提供数据机密性。AH 虽然在功能上和 ESP 有些重复, 但 AH 除了可以对 IP 的有效负载进行认证外, 还可以对 IP 头部实施认证。主要是在处理数据时, 可以对 IP 头部进行认证, 而 ESP 的认证功能主要是面对 IP 的有效负载。AH 既可以单独使用, 也可以和 ESP 联用。

本章介绍了 VPN 相关的几个协议, 为了避免混淆, 总结如下:

(1) **IPSec 协议。**IPSec 协议用来保证 IP 传输的安全, 包括 IP 头部和有效负荷的保护。至于使用什么加密算法进行加密, 使用什么 Hash 算法进行完整性检查, 与 IPSec 是独立的。IPSec 协议仅用来选择对什么进行保护, 如何保护则不属于 IPSec 协议的功能。

- **ESP:** 可以提供对有效负荷的加密、完整性检查、数据包内容的起源认证等。但不能对数据包的 IP 头部进行认证, 即无法验证地址起源。
- **AH:** 可以对 IP 头部进行认证, 也可以进行完整性检查和起源认证, 但不提供加密支持。

(2) **加密算法。**IPSec 中 ESP 可以选择的加密算法有 DES、3DES 和 AES。

(3) **认证。**提供数据的完整性检查和起源认证, 通过使用 Hash 算法确保数据没有被修改过, 也可以确保 IP 报头没有被修改过。使用的 Hash 算法有 MD5 和 SHA。

(4) **密钥交换算法 DH。**在通信两端建立密钥信息, DH 算法可以周期性地改变通信两端使用的密钥。使用的 DH 算法有 DH1、DH2 和 DH5。

19.3.5 VPN 配置*

这里介绍两种常见的 VPN 配置。

1. 站点到站点 (Site-to-Site) VPN 配置

实验 19-1: 使用 SDM 配置站点到站点 VPN

某公司总部和分部分别接入 Internet, 但总部和分部都只有一个公网 IP 地址, 如图 19-3-8 所示。要保证公司总部和分部的计算机都能访问 Internet; 因为办公需要, 公司总部和分部

的内部计算机要能安全互访。

分析：要保证内部很多计算机通过一个公网 IP 地址同时上网，这就要求在总部和分部的出口路由器上配置 NAT；要保证总部和分部的内部网络能够安全互访，这就需要配置总部到分部的 VPN，通过配置 VPN，既安全又节省费用。

图 19-3-8 中的拓扑可以抽象成图 19-3-9 中的实验拓扑。使用模拟器中的 R1、R2 和 R3，并在路由器 R1 和 R3 上各启用一个环回接口来模拟计算机。修改机架拓扑文件“labini/ccna.net”，增加 R1 和 R3 的内存到 128MB，以免配置中出现内存不足。通过命令行的方式配置 VPN，既复杂又容易出错。思科提供了 SDM 配置软件，通过图形化界面，很容易即可完成 VPN 的配置，且不容易出错。通过 SDM 配置软件，使用共享密钥建立站点到站点 VPN 的配置步骤如下：

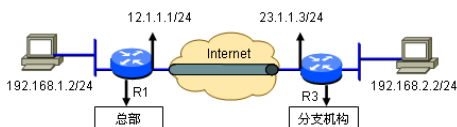


图 19-3-8 使用预共享密钥建立站点到站点 VPN

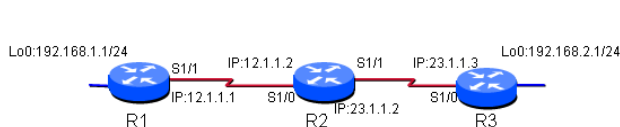


图 19-3-9 配置站点到站点 VPN

① 基本路由配置。配置路由器 R1、R2 和 R3 的接口 IP 地址，并配置静态路由，保证 R1、R2 和 R3 之间的公网 IP 地址可以互通。R1 的配置如下（斜体部分为注释）：

```
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0
配置这个以太网接口的目的是为了使用 SDM，把真实计算机的 IP 地址配置成 172.16.1.100/24，这样真实计算机就可以连接 R1 了。
R1(config-if)#ip add 172.16.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config)#int loopback 0
R1(config-if)#ip add 192.168.1.1 255.255.255.0 模拟一个私有网络。
R1(config-if)#no cdp run
R1(config)#ip http server 开启路由器的 http 服务，供 SDM 使用。
R1(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.2
```

R2 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
```

注意：R2 上不需要添加任何静态路由，因为 192.168 私有网段的地址是被 NAT 转换成公网地址后才发出来的，就像 Internet 上的路由器不会添加某个网络内部私有地址的路由一样。

R3 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
```

```
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config)#int fa 0/0
R3(config-if)#ip add 172.16.1.2 255.255.255.0
R3(config-if)#no shut
R3(config)#int loopback 0 模拟一个私有网络。
R3(config-if)#ip add 192.168.2.1 255.255.255.0
R3(config-if)#no cdp run
R3(config)#ip http server 开启路由器的 http 服务, 供 SDM 使用。
R3(config)#ip route 0.0.0.0 0.0.0.0 23.1.1.2
```

② 配置 NAT。有关 NAT 的配置请参照第 20 章的 NAT 部分, 这里仅给出配置和简单的解释。R1 的配置如下:

```
R1(config)#int lo0
R1(config-if)#ip nat inside 配置对内接口
R1(config-if)#int s1/1
R1(config-if)#ip nat outside 配置对外接口
R1(config-if)#exit
R1(config)#access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
因为 192.168.1.0/24 去往 192.168.2.0/24 的数据包不需要做地址转换, 它们之间的流量需要被加密, 走的是隧道, 隧道会在 IP 包中添加新的 IP 包头。
R1(config)#access-list 100 permit ip any any 除走隧道外的所有流量都允许被 NAT。
R1(config)#ip nat inside source list 100 interface s1/1 overload 内部私有地址使用 S1/1 接口的 IP 地址共享上网。
```

R3 的配置如下:

```
R3(config)#int lo0
R3(config-if)#ip nat inside
R3(config-if)#int s1/0
R3(config-if)#ip nat outside
R3(config)#access-list 100 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#access-list 100 permit ip any any
R3(config)#ip nat inside source list 100 interface s1/0 overload
```

至此, 路由器 R1 和 R3 环回接口的私有地址应该可以 ping 通所有的公共地址, 比如 12.1.1.1、12.1.1.2、23.1.1.2、23.1.1.3。但两台路由器环回接口之间的私有地址之间无法 ping 通。

③ 测试。在 R1 上使用环回接口的 IP 地址 192.168.1.1 去 ping 路由器 R2 的 23.1.1.3, 测试私有地址能否成功访问到公共地址。

在 R1 上要使用扩展 ping 命令, 如果直接使用 ping 命令, 路由器 R1 将使用离目标最近的接口, 也就是用 S1/1 接口的 IP 地址 12.1.1.1 去 ping。而这里要测试的是私有地址可以访问公共地址, 路由器 R1 的执行如下 (斜体部分为注释):

```
R1#ping
Protocol [ip]: ping 不添加地址, 直接回车。
Target IP address: 12.1.1.2 因为使用的是 IP 地址, 直接回车就可以了。
Repeat count [5]: 目标地址是 12.1.1.2。
Datagram size [100]: ping 包的数量。
Timeout in seconds [2]: 数据包包大小。
Extended commands [n]: y 超时时间, 默认为 2 秒。
Source address or interface: 192.168.1.1 是否要使用扩展命令, 一定要填 yes。
Type of service [0]: 使用哪个源地址或接口去 ping, 这里填入 Loopback 0 接口或接口的 IP 地址 192.168.1.1。
Set DF bit in IP header? [no]: 接下来的所有选项全部保持默认, 直接回车就可以了。
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.1.2, timeout is 2 seconds:
```

```
Packet sent with a source address of 192.168.1.1
!!!! 结果是可以 ping 通的。
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/26/44 ms
R1#
```

在 R2 上使用“debug ip icmp”命令，检验 R1 的扩展 ping 命令，R2 的显示结果如下，可以看出 R1 上的私有地址是转换成 12.1.1.1 后发送出去的。

```
R2#debug ip icmp
*May 29 10:11:41.047: ICMP: echo reply sent, src 12.1.1.2, dst 12.1.1.1
*May 29 10:11:41.303: ICMP: echo reply sent, src 12.1.1.2, dst 12.1.1.1
*May 29 10:11:41.447: ICMP: echo reply sent, src 12.1.1.2, dst 12.1.1.1
*May 29 10:11:41.739: ICMP: echo reply sent, src 12.1.1.2, dst 12.1.1.1
*May 29 10:11:41.879: ICMP: echo reply sent, src 12.1.1.2, dst 12.1.1.1
```

在 R1 上使用 192.168.1.1 去 ping R3 上的 192.168.2.1 失败。

④ 使用 SDM。在真实计算机上，双击桌面上的“Cisco SDM (Chinese Edition)”图标，输入路由器 R1 的 IP 地址 172.16.1.1，如图 19-3-10 所示。

单击“启动”按钮，打开后的 SDM 主界面如图 19-3-11 所示。从该界面中可以看到路由器的型号、内存和闪存大小、IOS 的版本、SDM 的版本、支持的功能（包括 IP、防火墙、VPN、IPS、NAC）等。



图 19-3-10 SDM 连接路由器

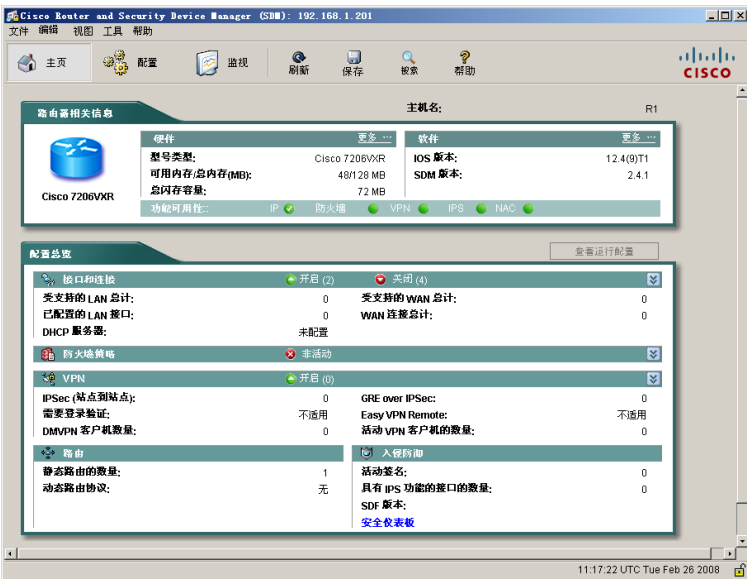


图 19-3-11 SDM 主界面

⑤ 启动 VPN 向导。单击 SDM 主界面工具栏中的“配置”图标→左侧导航栏中的“VPN”图标→中间栏中的“站点到站点 VPN”，选中右侧窗口中的“创建站点到站点 VPN”，单击“启动选定的任务”按钮，如图 19-3-12 所示，打开 VPN 配置向导。

⑥ 逐步操作向导。在“站点到站点 VPN 向导”中，选择“逐步操作向导”，如图 19-3-13 所示。单击“下一步”按钮。

⑦ VPN 连接信息。在“VPN 连接信息”对话框中，如图 19-3-14 所示，为 VPN 连接选择接口，这里选择“Serial 1/1”；在“对等项标识”栏中选择“有静态 IP 地址的对等项”，并填入远程对等项的 IP 地址 23.1.1.3；在“验证”方式栏中选择“预共享密钥”，并填入共享密钥，假设是 cisco。单击“下一步”按钮继续。



图 19-3-12 配置 VPN 向导

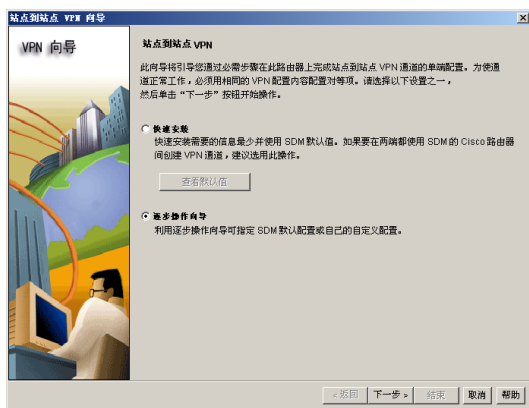


图 19-3-13 逐步操作向导



图 19-3-14 “VPN 连接信息”对话框

⑧ IKE (Internet Key Exchange, Internet 密钥交换) 提案。这里要配置的是一个策略，使用什么样的方式来保证密钥的安全。这里使用默认的策略集，如图 19-3-15 所示，如果不满意，可以单击“添加”按钮，添加新的策略集。单击“下一步”按钮继续。

⑨ 转换集。这里配置的是数据加密的方法，默认使用的是 ESP 协议，3DES 加密，哈希算法使用的是 SHA，如图 19-3-16 所示。单击“下一步”按钮继续。

⑩ 要保护的通信。在图 19-3-17 中，配置要保护的通信，选择“保护下列子网间的所有通信”，在本地网中填入 192.168.1.0/24，在远程网中填入 192.168.2.0/24。也可以选择“创建/选择 IPSec 通信的访问列表”。单击“下一步”按钮继续。



图 19-3-15 配置 IKE

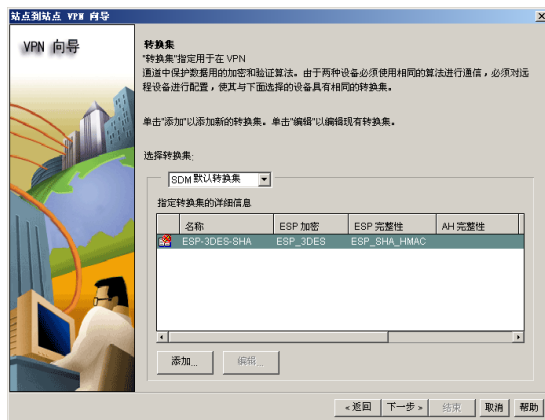


图 19-3-16 配置转换集



图 19-3-17 配置要保护的通信

① 完成配置。单击“完成”按钮，结束 VPN 配置向导，向导会提示一些不兼容问题，如图 19-3-18 所示，单击“是”按钮，接受修改就可以了。

SDM 弹出如图 19-3-19 所示的对话框，SDM 把配置命令上传到路由器。

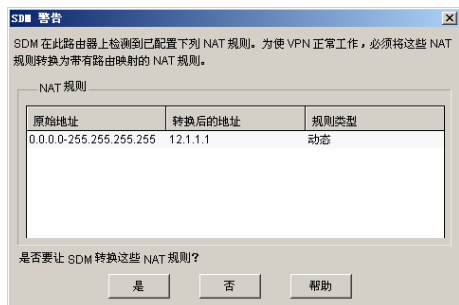


图 19-3-18 SDM 警告

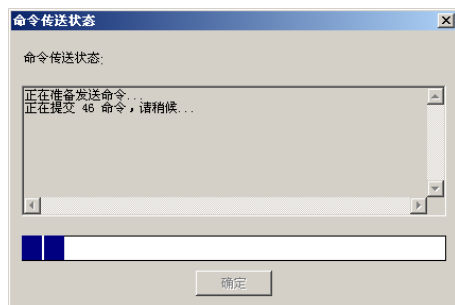


图 19-3-19 上传配置

② 配置路由器 R3。操作过程与 R1 类似，在如图 19-3-14 所示的界面中选择“Serial 1/0”

接口，远程对等体的 IP 地址填入 12.1.1.1，两边填入相同的密钥。在如图 19-3-17 所示的界面中，把本地网和远程网反过来填写。

⑬ 测试 VPN 通道。在路由器 R1 上使用扩展的 ping 命令，源 IP 地址是 192.168.1.1，目标 IP 地址是 192.168.2.1，如下所示，可以发现能够 ping 通了，第一个数据包没通的原因是因为 VPN 隧道还没有建立起来，第一个包的流量触发了隧道建立。

```
R1#ping
Protocol [ip]:
Target IP address: 192.168.2.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 28/43/60 ms
```

在 R3 上使用“debug ip icmp”命令，检验 R1 的扩展的 ping 命令，R3 的显示结果如下，可以看出来源地址是 R1 上的私有地址 192.168.1.1。

```
R3#
*Mar 1 01:11:31.699: ICMP: echo reply sent, src 192.168.2.1, dst 192.168.1.1
*Mar 1 01:11:31.759: ICMP: echo reply sent, src 192.168.2.1, dst 192.168.1.1
*Mar 1 01:11:31.799: ICMP: echo reply sent, src 192.168.2.1, dst 192.168.1.1
*Mar 1 01:11:31.851: ICMP: echo reply sent, src 192.168.2.1, dst 192.168.1.1
```

2. Easy VPN 配置

有时也称做远程 VPN，远程 VPN 主要用来为移动用户或 SOHO 用户服务，中心站点需要有支持 VPN 的设备并分配有固定的 IP 地址，远程站点或移动用户不需要有固定的 IP 地址。对于移动用户来说，通过在客户端计算机上安装 VPN 软件，连基本的 VPN 设备也不需要了。客户端通过中心站点提供的 VPN 设备 IP 地址、组名、组密码、用户名和用户密码等参数连接到中心站点的 VPN 设备，建立从客户端到中心站点设备间的 VPN 隧道，保证数据传输的安全。有关远程 VPN 的配置，本书不作过多介绍，感兴趣的读者可以参阅 CCNP 课程中的远程部分。



19.4 真题精选*

本章相关的内容目前还没有出现在 CCNA 的考试中，但并不表示将来不会出现。下面列出的两个 VPN 拖拉题来自于思科官方网站。

1. In this activity, a simulation is provided of a small company that has setup Internet connectivity using two Linksys WRVS4400N business class routers. One is located at the Central site and the other at the Branch site. They would like to access resources between sites but are concerned that the Internet traffic would not be secure. To address their concern, it has been suggested that they implement a site-to-site VPN between the two

sites. A VPN would enable the Branch site office to connect to the Central site office securely by creating a VPN tunnel which would encrypt and decrypt data.

Referencing the topology, you will use the Linksys router's web configuration utility to configure the settings and enable a VPN called Site-to-Site using MD5 authentication, 3DES encryption, and a pre-shared key of cisco123.

The diagram illustrates a Site-to-Site VPN setup between a Central Site and a Branch Site. The Central Site has a LAN of 192.168.1.0/24 and a WAN interface with IP 209.165.200.225. The Branch Site has a LAN of 192.168.101.0/24 and a WAN interface with IP 209.165.202.129. They are connected via the Internet. Below the diagram, two screenshots of the Linksys router's web configuration utility show the IPsec VPN configuration for both sites. The configuration includes fields for Local/Remote Security Groups, Tunnel Name, IPsec VPN Tunnel, Local/Remote Security Group Type, IP Address, Subnet Mask, Remote Security Gateway Type, Key Exchange Method, Encryption, Authentication, PFS, Pre-Shared Key, and Key Life Time. A sidebar on the right lists various VPN options like MD5, Site-to-Site, 192.168.101.0, 209.165.202.129, 192.168.1.0, 3DES, Cisco1233, cisco123, 192.168.1.1, 209.165.200.0, 209.165.202.0, DES, AES, SHA, and Remote Access.

2. A small company that has setup Internet connectivity using a Linksys WRVS4400N business class router at their Central site. They would like to provide remote access to select users from remote locations but are concerned that the Internet traffic would not be secure. To address this concern, it has been suggested that they implement a remote access VPN which would allow telecommuters to securely access the Central site network. Using the Linksys Quick VPN client software, remote users would be able to connect and establish a remote access VPN connection which would encrypt and decrypt data.

Referencing the topology, you will use the Linksys routers web configuration utility to configure the remote VPN settings and configure a user account. The user's name is BobV and his

password is cisco123.

Next, Bob will initiate a remote VPN connection to the Central site router using the Linksys QuickVPN client software. The profile name should be Central Site and the correct username , password and IP address should be referenced .



19.5 真题解答*

1. 有一个小公司使用了两台 Linksys WRVS4400N 的路由器建立了 Internet 连接。一端在中心站点，另一端在分支机构。两个站点之间想互相访问资源，但考虑到 Internet 的不安全性，为了解决这个问题，建议在两个站点之间配置站点到站点的 VPN。VPN 可以在分支机构和中心站点之间创建一个 VPN 隧道来加密和解密数据。

参照拓扑结构，你将使用 Linksys 路由器的 Web 配置工具来配置设备，使用 MD5 认证，

3DES 加密，预共享密钥 cisco123 来建立站点到站点的 VPN。借鉴实验 19-1，正确的配置如下图所示。

The image shows two identical configuration windows for a Cisco VPN setup, one for the Central site and one for the Branch site. The configuration includes:

- Select Tunnel Entry:** --new--
- Local Security Group:** IPsec VPN Tunnel: Enable, Tunnel Name: Site-to-Site
- Remote Security Group:** Local Security Group Type: Subnet, IP Address: 192.168.1.0, Subnet Mask: 255.255.255.0
- Remote Security Gateway:** Remote Security Group Type: Subnet, IP Address: 192.168.1.0, Subnet Mask: 255.255.255.0
- Key Management:** Remote Security Gateway Type: P. Addr, IP Address: 209.165.202.129
- Advanced:** Key Exchange Method: Auto (IKE), Encryption: 3DES, Authentication: MD5, PFS: Enable, Pre-Shared Key: cisco123, Key Life Time: 28800 Sec.

On the right side of each window, there is a list of IP addresses and a 'Remote Access' button. For the Central site, the list includes 192.168.1.1, 192.168.101.1, 209.165.200.0, 209.165.200.225, 209.165.202.0, and 209.165.202.129. For the Branch site, the list includes 209.165.202.129, 192.168.1.1, 192.168.101.1, 209.165.200.0, 209.165.202.0, and 209.165.202.129.

2. 一个小公司在中心站点使用 Linksys WRVS4400N 路由器连接到 Internet，他们希望能够给远程地点中的选择用户提供安全的远程接入，但 Internet 不安全，为了解决这一问题，建议用快速的 Linksys VPN 客户端软件配置远程访问 VPN，这将使远程安全访问中心站点的网络，远程用户将能够连接和建立一个远程访问 VPN 用来加密和解密数据。

参照拓扑结构，你将使用 Linksys 路由器的 Web 配置实用程序配置远程 VPN 以及配置用户账号。用户名是 BobV，密码是 cisco123。

接下来，Bob 将使用 Linksys 快速 VPN 客户端软件启动远程 VPN 连接到中心站点的路由器。使用中心站点的用户名、密码和 IP 地址作为参照。

The image shows two screenshots of the Linksys VPN configuration interface. The left screenshot is the 'VPN' tab in the Linksys Web Configuration Utility, showing a table of users and a list of IP addresses. The right screenshot is the 'Linksys VPN Client' window, showing fields for Profile Name, User Name, Password, and Server Address.

Linksys Web Configuration Utility - VPN Tab:

No.	Active	Username	Password	Edit	Remove
1	<input checked="" type="checkbox"/>	BobV	cisco123	Edit	Remove
2	<input type="checkbox"/>			Edit	Remove
3	<input type="checkbox"/>			Edit	Remove
4	<input type="checkbox"/>			Edit	Remove
5	<input type="checkbox"/>			Edit	Remove

Linksys VPN Client:

Profile Name: Central Site
 User Name: BobV
 Password: cisco123
 Server Address: 209.165.202.225

Buttons: Connect, Save, Delete, Help

第 20 章

DHCP 和 NAT***

本章主要介绍 DHCP (Dynamic Host Configuration Protocol, 动态主机分配协议) 和 NAT (Network Address Translation, 网络地址转换)。通过把路由器配置成 DHCP 服务器, 实现内部主机 IP 地址的动态分配; 把路由器配置成 NAT 设备, 仅用一个或有限的几个公共 IP 地址实现内部主机的共享上网, 以及对外提供网络服务。本章在 CCNA 考试中占有相当比重, 尤其是 NAT 部分占的比重更大。本章在实际工程中应用较多, 建议读者多加练习, 熟练掌握。



20.1 DHCP**

DHCP 是一个简化主机 IP 地址分配管理的 TCP/IP 标准协议。用户可以利用 DHCP 服务器管理动态的 IP 地址分配及其他相关的环境配置工作 (如 DNS、WINS、Gateway 的设置等)。

在使用 TCP/IP 协议的网络上, 每一台计算机都拥有唯一 IP 地址。当用户将计算机从一个子网移动到另一个子网的时候, 一定要改变该计算机的 IP 地址。如果采用静态 IP 地址的分配方法, 将增加网络管理员的负担, 而 DHCP 可以让用户将 DHCP 服务器中 IP 地址数据库中的 IP 地址动态地分配给局域网中的客户机, 从而减轻了网络管理员的负担。

20.1.1 使用 DHCP 的好处**

使用 DHCP 的好处主要有以下两点:

- DHCP 避免了因手工设置 IP 地址及子网掩码所产生的错误, 同时也避免了把一个 IP 地址分配给多台工作站所造成的地址冲突。
- 使用 DHCP 服务器大大缩短了配置或重新配置网络中工作站所花费的时间, 同时通过对 DHCP 服务器的设置可灵活地设置地址的租期。DHCP 地址租约的更新过程将有助于用户确定哪个客户的设置需要经常更新 (如: 使用便携机的客户经常更换地点), 且这些变更由客户机与 DHCP 服务器自动完成, 无须网络管理员干预。

20.1.2 BOOTP 和 DHCP 的区别与联系**

BOOTP (Bootstrap Protocol) 比 DHCP 出现得早, 和 DHCP 有一些类似的处理过程。BOOTP 主要用于无盘工作站。无盘工作站没有硬盘和操作系统, 但维护方便, 很多超市的收银终端使用的就是这种工作站。DHCP 和 BOOTP 都基于客户/服务模式, 都使用 UDP 的 67 和 68 号端口。

在 DHCP 和 BOOTP 中，服务器负责 IP 地址的分配和管理，每一个分配的 IP 地址都存储在服务器的数据集中，叫做捆绑（binding）；客户端使用 DHCP 获取 IP 地址信息。

DHCP 和 BOOTP 主要有 3 点不同：

- 最主要的不同是，BOOTP 中预先手工配置主机信息，当 BOOTP 客户端请求 IP 地址时，BOOTP 服务器在预先配置的信息表中搜索和请求客户端 MAC 地址相匹配的条目。如果该条目存在，和这个条目相对应的 IP 地址被返回给客户端。这意味着 IP 地址和 MAC 地址的捆绑条目必须被预先配置在 BOOTP 服务器上。
- DHCP 根据租约机制允许客户端续租或重新分配网络地址。这种租约机制允许一个 IP 地址在不同的时间可以被分配给多个客户端使用，也允许一个客户端移到另一个子网时重新获取新的 IP 地址，还允许客户端刷新租约或保持相同的 IP 地址。BOOTP 不使用租约机制，BOOTP 中一个客户端被分配的 IP 地址不能再被分配给其他的客户端。
- BOOTP 只能分配 4 个参数：IP 地址、子网掩码、网关、DNS。DHCP 除了提供 4 个基本的参数外，还可以提供额外的配置参数，诸如 WINS 和域名等。

20.1.3 DHCP 工作过程**

思科多数文档关于本节的叙述都有错误，为了让大家能更深入地理解 DHCP 工作过程，这里结合 Sniffer 抓包，给大家分析 IP 地址的获取过程。

实验 20-1：捕获 DHCP 数据包，分析 IP 地址获取全过程

1. 捕获包

① 为了便于分析，把计算机连接到一台单独的交换机或集线器上，关闭计算机上无关的应用程序，这样做的目的是仅捕获相关的包。

② 运行 CCNA 机架中的 R1 和 R2。R1 的配置如下（斜体部分是注释）：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#no cdp run
R1(config)#int fa 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
接下来这段是 DHCP 服务器的配置。
R1(config)#ip dhcp excluded-address 192.168.1.1 排除 192.168.1.1，把网关排除出地址池。
R1(config)#ip dhcp pool nat-pool 配置 DHCP 地址池 pool，名字叫 nat-pool。
R1(dhcp-config)#network 192.168.1.0 /24 分配 192.168.1.0 网段地址，掩码是 24 位。
R1(dhcp-config)#default-router 192.168.1.1 网关是 192.168.1.1。
R1(dhcp-config)#dns-server 218.2.135.1 DNS 服务器的地址是 218.2.135.1。
```

R2 的配置如下：

```
Router#conf t
Router(config)#host R2
R2(config)#no cdp run
R2(config)#int fa 0/0
R2(config-if)#ip address dhcp
```



注意：先不要打开 R2 的 Fa0/0 端口。

③ 运行 Sniffer 软件，并开始抓包。

- ④ 打开 R2 的 Fa0/0 端口。
- ⑤ 当 R2 的屏幕出现如图 20-1-1 所示的信息时，停止 Sniffer 的包捕获。

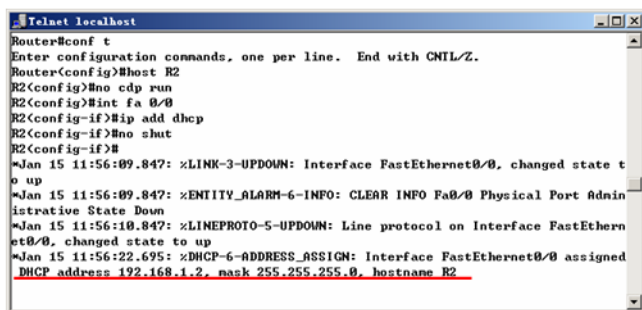


图 20-1-1 路由器获取 IP 地址

⑥ Sniffer 捕获的包如图 20-1-2 所示。这里捕获的数据包被保存在光盘中的“配置\20\sniffer-dhcp.cap”文件中，读者可以用 Sniffer 打开该文件，查看报文内容。如果计算机上还有其他应用程序发包，可能会夹杂其他的数据包，但图中的 6 个包应该都在。

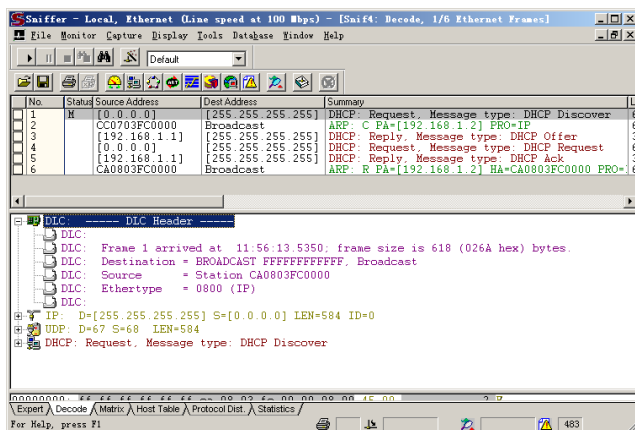


图 20-1-2 Sniffer 捕获的包

2. 分析包

当 DHCP 客户机启动登录网络时，通过以下步骤从 DHCP 服务器获得租约。

① DHCP 客户机 (R2) 在本地子网中先发送 DHCP Discover 信息，此信息以广播的形式发送，因为客户机现在还不知道 DHCP 服务器的 IP 地址。该数据包的源 MAC 地址是路由器 R2 Fa0/0 端口的 MAC 地址，目的 MAC 地址是“FFFFFFFFFFFF”，广播 MAC 地址；该数据包的源 IP 地址是“0.0.0.0”，因为路由器 R2 现在还没有 IP 地址，目的 IP 地址是“255.255.255.255”，因为路由器 R2 并不知道 DHCP 服务器的 IP 地址，只能广播发送；DHCP 使用的是 UDP 协议，客户端的端口号是 68，服务器端使用的端口号是 67；数据包的用途是“DHCP Discover”。该数据包是图 20-1-2 中的第一个包。

② DHCP 服务器 (R1) 收到 DHCP 客户机广播的 DHCP Discover 信息后，它发现有一个 IP 地址“192.168.1.2”可以被租用。DHCP 服务器提供租用地址前，首先要发送一个 ARP 查询包，查询“192.168.1.2”在网络上有没有被使用，如果收到 ARP 应答包，表明该 IP 地

址在网络上已经被使用，DHCP 服务器在地址池中换一个地址再试；如果没有收到 ARP 应答包，表明该 IP 地址没有被使用。ARP 查询包也是一个广播包，源 MAC 地址是 R1 路由器 Fa0/0 端口的 MAC 地址，目的 MAC 地址是广播 MAC 地址，ARP 查询包的源 IP 地址是“192.168.1.1”，ARP 查询包的目的地 IP 地址是“192.168.1.2”。该数据包是图 20-1-2 中的第二个包。

③ DHCP 服务器向 DHCP 客户机发送 DHCP Offer 信息，其中包括一个可租用的 IP 地址。该数据包仍然是一个广播包，源 MAC 地址是 DHCP 服务器的 MAC 地址，目的 MAC 地址是广播 MAC 地址（很多文档都解释成单播 MAC 地址，认为 DHCP 服务器直接给 DHCP 客户端发包就可以了。其实不然，DHCP 服务器还要通知网络上的其他 DHCP 服务器，这样设计主要是考虑同一个网段有多个 DHCP 服务器的情况。有关这一点可以在图 20-1-3 中得到验证）；源 IP 地址是 DHCP 服务器的 IP 地址“192.168.1.1”，目的 IP 地址是广播 IP 地址“255.255.255.255”，因为此时 DHCP 客户端仍没有 IP 地址；传输层使用的仍然是 UDP 协议，源端口号变成了 67，目的端口号是 68；DHCP Offer 中包含了要分配给客户端的 IP 地址和客户端的 MAC 地址。

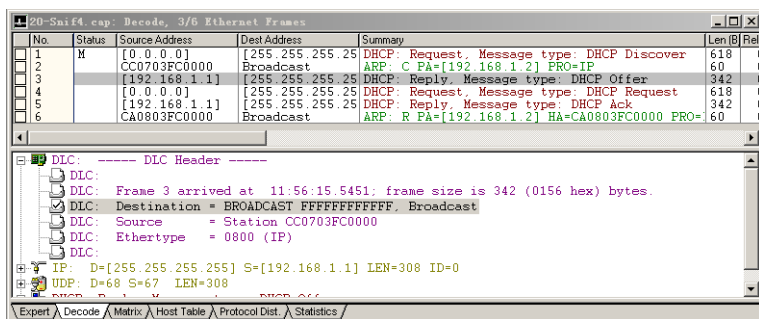


图 20-1-3 DHCP Offer 信息

如果没有 DHCP 服务器对客户机的请求做出反应，则客户机无法获得 IP 地址，初始化失败。但客户机在后台会每隔一段时间发送几个 DHCP Discover 信息，直到它收到 DHCP Offer 信息。如果是 Windows 的客户端，多次尝试失败后，客户机将会被分配 169.254.0.0/16 的 IP 地址，但客户端仍会继续尝试联系 DHCP 服务器，一旦找到 DHCP 服务器，客户端会使用新获取的 IP 地址替换 169.254.0.0/16 的 IP 地址。

④ 客户机收到 DHCP Offer 信息，它发送 DHCP Request 租约选择信息到服务器，表示它将使用服务器所提供的 IP 地址。该数据包仍然是一个广播包，源 MAC 地址是 DHCP 客户端的 MAC 地址，目的 MAC 地址是广播 MAC 地址（很多文档都解释成单播 MAC 地址，认为 DHCP 客户端直接给选择的 DHCP 服务器发包就可以了。其实不然，DHCP 客户端还要通知网络上的其他 DHCP 服务器，它选择了某个 IP 服务器分配的某个 IP 地址，其他服务器也会收到这个信息，其他服务器把分配出去的 IP 地址收回到地址池中。这样设计也是考虑到同一个网段有多个 DHCP 服务器的情况。读者可以按图 20-1-4 所示方法进行验证）；源 IP 地址是 DHCP 客户端的 IP 地址“0.0.0.0”，因为此时 DHCP 客户端仍没有 IP 地址，目的 IP 地址是广播 IP 地址“255.255.255.255”；传输层使用的仍然是 UDP 协议；DHCP Request 中包含了要选择的服务器和客户端要使用的 IP 地址。

⑤ DHCP 服务器在收到 DHCP 租约选择信息后，即发送 DHCP Ack 确认信息，以确定

此租约成立，且此信息中还包含其他 DHCP 选项信息，比如掩码、网关、DNS 等。该数据包仍以广播发送。

⑥ 客户机收到确认信息后，利用其中的信息配置它的 TCP/IP 属性。发送一个 ARP Reply 包通知网络上的其他设备，该 IP 地址已经被使用。

综上所述，DHCP 的工作过程如图 20-1-5 所示，即 IP 租约请求、IP 租约提供、IP 租约选择、IP 租约确认。

No.	Status	Source Address	Dest Address	Summary	Len	Rel
1	H	[0.0.0.0]	[255.255.255.255]	DHCP: Request, Message type: DHCP Discover	618	
2		CC0703FC0000	Broadcast	ARP: C FA=[192.168.1.2] PRO=IP	60	
3		[192.168.1.1]	[255.255.255.255]	DHCP: Reply, Message type: DHCP Offer	342	
4		[0.0.0.0]	[255.255.255.255]	DHCP: Request, Message type: DHCP Request	618	
5		[192.168.1.1]	[255.255.255.255]	DHCP: Reply, Message type: DHCP Ack	342	
6		CA0803FC0000	Broadcast	ARP: R FA=[192.168.1.2] HA=CA0803FC0000 PRO=	60	

图 20-1-4 DHCP Request 信息



图 20-1-5 DHCP 的工作过程

20.1.4 配置 DHCP 服务器和客户端***

本节通过实验 20-2 讲解路由器充当 DHCP 服务器的配置、路由器和计算机充当 DHCP 客户端的配置、DHCP 配置的验证和测试。实验拓扑如图 20-1-6 所示，路由器 R1 充当 DHCP 服务器，对虚拟的 PC1 和真实计算机分配 IP 地址，并测试虚拟的 PC1 与真实计算机的连通性。

实验 20-2: DHCP 配置及测试

运行 CCNA 机架中的 PC1、SW1、R1。注意：即使 SW1 不用配置，也要登录 SW1 的控制台，激活所有的端口，不然 PC1 到 R1 链路不通。

1. 配置 DHCP 服务器

路由器 R1 的配置如下（斜体部分是注释）：

```
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int fa 2/0
1(config-if)#ip add 192.168.2.1 255.255.255.0
R1(config-if)#no shut
R1(config)#ip dhcp pool pool1
R1(dhcp-config)#network 192.168.1.0 /24
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#dns-server 202.102.3.141
R1(dhcp-config)#domain-name test.com
R1(dhcp-config)#lease 8
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 192.168.1.1
```

配置 DHCP 地址池，名字是 pool1。
分配 192.168.1.0 网段地址，掩码是 24 位。
网关是 192.168.1.1。
DNS 服务器的地址是 202.102.3.141。
主机的域名是 test.com。
IP 地址租期是 8 天，默认是无限期。
还有很多可选信息，这里只配置常用的。

排除 192.168.1.1，把网关排除出地址池。

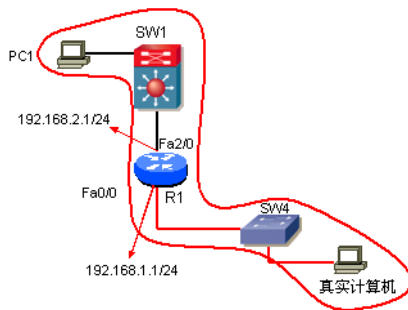


图 20-1-6 DHCP 配置


```
R1(config)#ip dhcp pool pool2
R1(dhcp-config)#network 192.168.2.0 /24
R1(dhcp-config)#default-router 192.168.2.1
R1(dhcp-config)#dns-server 202.102.3.141
R1(dhcp-config)#domain-name test.com
R1(dhcp-config)#lease 8
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 192.168.2.1
```

配置 DHCP 地址池，名字是 pool2。

2. 虚拟 PC1 的配置如下（斜体部分是注释）：

```
PC1(config)#int fa 0/0
PC1(config-if)#ip address dhcp //配置 DHCP。
PC1(config-if)#no shut
PC1(config-if)#exit
PC1(config)#no ip routing //路由器模拟 PC，需关闭路由协议，不然默认网关不起作用。
```

3. 配置真实计算机

如图 20-1-7 所示，把计算机的 IP 地址设成自动分配。

4. 测试

① 真实计算机测试。在真实计算机上执行“ipconfig /all”命令，查看 IP 地址分配情况，结果如图 20-1-8 所示。

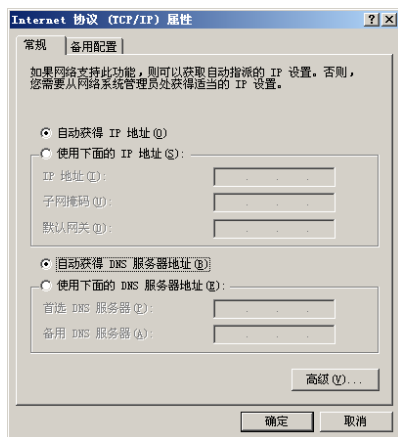


图 20-1-7 配置计算机自动获得 IP 地址

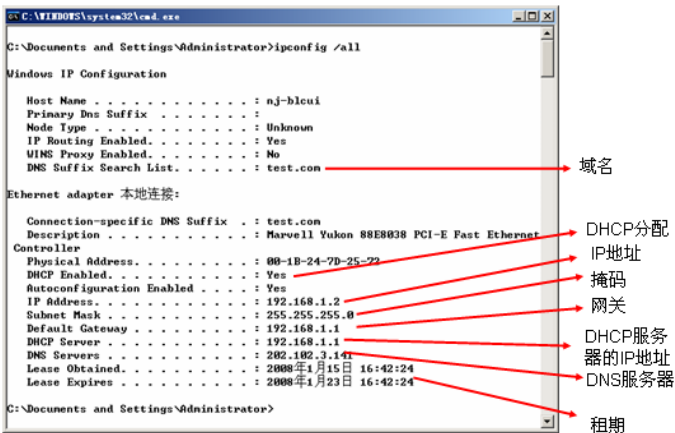


图 20-1-8 计算机作为 DHCP 客户端

② 虚拟 PC1 测试。在 PC1 上执行“show ip route”和“show ip int brief”命令，“ping 192.168.1.2”（真实计算机获取到的 IP 地址），结果如图 20-1-9 所示。

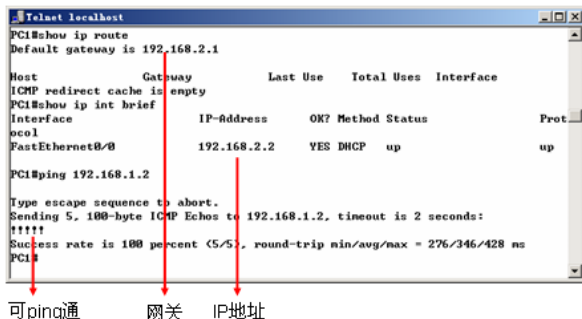


图 20-1-9 路由器作为 DHCP 客户端

③ DHCP 服务器测试。在路由器 R1 上执行“show ip dhcp binding”命令，查看 IP 地址的分配情况；执行“show ip dhcp server statistics”命令，查看 DHCP 服务器的状态；执行“show ip dhcp pool”命令，查看地址池的情况。

20.1.5 配置 DHCP 中继服务*

在复杂的层次型网络中，企业的服务器经常集中存放在服务器区。此时问题出现了，DHCP 客户端和 DHCP 服务器不在同一个网段，DHCP 客户端的广播包被三层设备阻止，无法到达 DHCP 服务器，DHCP 客户端获取地址失败。

实验 20-3：配置 DHCP 中继

在图 20-1-10 中，真实计算机需要从 R2（DHCP 服务器 23.1.1.2）上获取 IP 址。

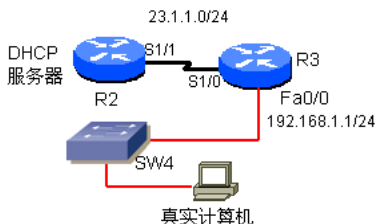


图 20-1-10 DHCP 中继

① R2 和 R3 的配置如下（斜体部分是注释）：

```
R2(config)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config)#ip dhcp pool pool1
R2(dhcp-config)#network 192.168.1.0 /24
R2(dhcp-config)#default-router 192.168.1.1 //不要误认为这里是 23.1.1.2，真实计算机
//的网关是路由 R3 Fa0/0 端口的 IP 地址。

R2(dhcp-config)#dns-server 202.102.3.141
R2(dhcp-config)#exit
R2(config)#ip route 192.168.1.0 255.255.255.0 23.1.1.3

R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int fa 0/0
R3(config-if)#ip add 192.168.1.1 255.255.255.0
R3(config-if)#no shut
```

② 配置真实计算机动态获取 IP 地址。如果之前计算机已经是动态获取的 IP 地址，需在 DOS 窗口中输入“ipconfig /release”命令，释放先前获取到的 IP 地址；输入“ipconfig /renew”命令，重新获取 IP 地址。计算机提示获取 IP 地址失败，输入“ipconfig /all”命令，看到计算机的 IP 地址是“169.254.0.0/16”，这表明 DHCP 客户端找不到 DHCP 服务器。失败的原因是因为路由器 R3 并没有把真实计算机的 DHCP Discover 包转发给路由器，三层设备有隔离广播的作用。解决的办法可以是在每个网段都架设一台有 DHCP 服务功能的设备，可这样做的花费大且不利于集中维护和管理。

③ 配置 DHCP 中继。对于上述问题的另一种解决办法是配置连接 DHCP 客户端的那台路由器或三层交换机的辅助寻址功能，让三层设备充当 DHCP 中继，代为转发 DHCP 请求。配置 R3 的 DHCP 中继功能：

```
R3(config)#int fa 0/0 //不管 DHCP 客户端和 DHCP 服务器之间经过多少台设备，只需配置离 DHCP
//客户端最近的那个以太网接口即可。
R3(config-if)#ip helper-address 23.1.1.2 //把收到的 DHCP 广播包以单播的方式转发到服务器
//23.1.1.2。
```

DHCP 不是被路由器中继的唯一服务，在默认情况下，路由器会转发 8 个 UDP 服务：

- Port 37: Time
- Port 49: TACACS

- Port 53: DNS
- Port 67: DHCP/BOOTP client
- Port 68: DHCP/BOOTP server
- Port 69: TFTP
- Port 137: NetBIOS name service
- Port 138: NetBIOS datagram service

如果需要转发额外的端口，可以使用“ip forward-protocol”命令指定转发的协议和端口号。

④ 在真实计算机上，再次执行“ipconfig /renew”命令，发现可以成功获取到 IP 地址。

20.1.6 使用 SDM 配置 DHCP

SDM 中也支持 DHCP 服务器的配置，如图 20-1-11 所示，按照图中标识顺序单击“Configure”→“Additional Tools”→“DHCP Pools”→“Add”，在打开的窗口中，按如图 20-1-12 所示进行填写。DHCP Pool Name（DHCP 地址池的名字）是 pool1；DHCP Pool Network（DHCP 地址池分配的网络号）是 192.168.1.0；Subnet mask（子网掩码）是 255.255.255.0；DHCP 的起始 IP 地址是 192.168.1.2，结束 IP 地址是 192.168.1.254，其间排除了网关的 IP 地址；Lease Length（租期）是 8 天；在 DHCP Options（DHCP 选项）中，DNS 服务器是 202.102.3.141，域名是 test.com，网关是 192.168.1.1。

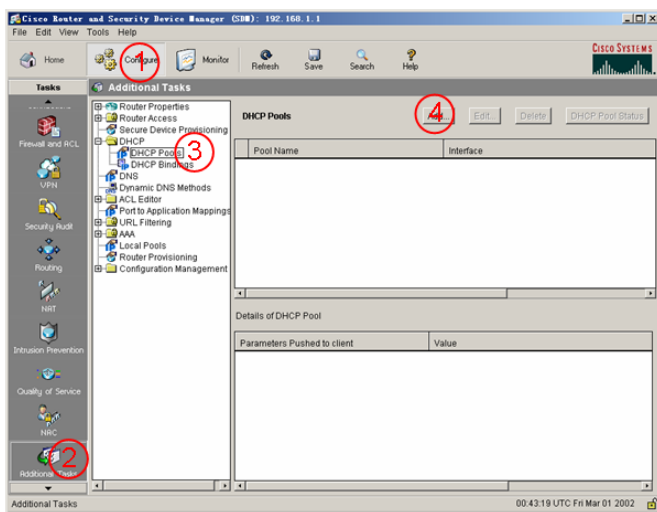


图 20-1-11 使用 SDM 配置 DHCP

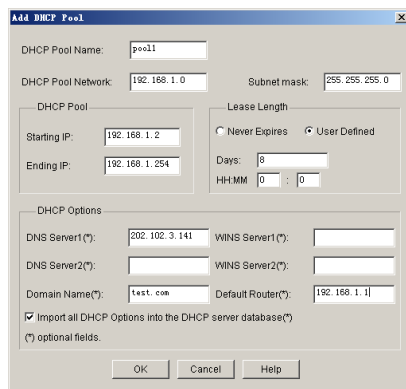


图 20-1-12 在 SDM 中配置 IP 地址池



20.2 NAT***

随着 Internet 的迅速发展，IP 地址短缺已成为一个十分突出的问题。为了解决这个问题，出现了多种解决方案。下面介绍一种在目前网络环境中比较有效的方法 NAT（Network Address Translation，网络地址转换）。

20.2.1 私有地址和公共地址***

Internet 协议要求网络上的每个网络接口都有一个唯一的地址。如果网络的范围是全球

性的，则地址也必须是全球唯一的，这就是 Internet。由于要保证全球的唯一性，所以必须有一个集中的授权组织负责正确、公平地分配 IP 地址。在近几年里，上述工作都是由 IANA (Internet Assigned Numbers Authority, Internet 编号分配机构) 来完成的。随着 Internet 在网络数量和应用数量上一直呈现快速增长的趋势，到 20 世纪 90 年代，Internet 商业化和国际化趋势已经出现。为了满足日益增长的 Internet 用户需求，目前，Internet 域名网号分配公司 (ICANN) 正式取代了 IANA。

如果一个组织希望在他的网络中使用 IP 协议和应用，但并不打算连接到 Internet 上，此时他所使用的 IP 地址可以不是全球唯一的，这种类型的网络叫做私有网络。如果某单位正在一个私有网上使用 IP 地址，只要遵守一般的 IP 地址管理规则，就可以任意选择 IP 地址。在随意分配 IP 地址时，首先要考虑下面的可能性：

- 事实上大部分组织都将实现与 Internet 进行某种连接，至少要使用电子邮件。
- 未来的合并或需求可能需要将网络加入一个或多个其他网络中。

例如，假设一个单位需要一个 C 类地址，但这个单位不需要连接到 Internet，随便选择 202.119.248.0/24 作为网络地址，然后按要求配置网上的所有设备。当一切设置完成后，单位领导又决定要接入 Internet。单位网管马上去咨询 ISP (Internet Service Provider, Internet 服务提供商)，ISP 告诉网管不要担心，可以使用一种网络地址转换技术来保持用户现有网络地址不变，并能够访问 Internet。接入 Internet 后，除了不能访问 “*.njut.edu.cn”，其他任何访问均正常，因为 C 类地址 202.119.248.0 已经被正式分配给南京工业大学，并且服务器被分配在这个网段。当试图访问某个 Web 站点，比如 www.njut.edu.cn 时，DNS 会对域名进行解析，得到的 IP 地址是 202.119.248.65。单位内的计算机认为（也正是这样）这个 IP 地址在单位内部的网络中，不会将这个数据包转发给路由器。讲到这里我们可以看到，随意选择 IP 地址是有一定风险的，除非能绝对保证永远不连接到 Internet。

考虑到上述情况，RFC 提出了一种有助于保留全球唯一 IP 地址的方法，这种方法使用了 3 个保留地址块。这 3 块地址永远不会分配给任何组织，这些地址块能够被用到任意私有网中，而不用担心官方分配给其他组织的 IP 地址与此块地址相重叠。

RFC1918 将下面 3 个地址范围作为私有地址块：

- 10.0.0.0~10.255.255.255
- 172.16.0.0~172.31.255.255
- 192.168.0.0~192.168.255.255

第一个块等价于传统的 A 类地址。如果使用 CIDR 符号进行描述的话，它的值应为 10.0.0.0/8。由于在 32 位中有 8 位是固定的，所以 RFC1918 将这个地址块叫做 24 位地址块。也就是说，这 24 位可由本地管理，它所包含的地址数量多达 $16777216 (2^{24})$ 个，足够一个大型网络使用。

第二个块被叫做 20 位地址块，等价于 16 个传统 B 类网络。如果使用 CIDR 符号进行描述的话，它的值应为 172.16.0.0/12。这个块包含 1048576 个 IP 地址。

第三个块被叫做 16 位地址块，等价于 256 个 C 类网络。如果使用 CIDR 符号进行描述的话，它的值应为 192.168.0.0/16。这个 16 位的前缀能够提供 $65536 (2^{16})$ 个 IP 地址。

除了上述私有地址段外，通常所说的 A、B、C 类地址都是公共地址，公共地址的使用需要向相关机构进行申请。D 类是组播地址，E 类用于科研，D 类和 E 类不属于通常所说的公共地址。

20.2.2 什么是 NAT***

NAT 提供了连接互联网的一种简单方式，并且通过隐藏内部网络地址的手段为用户提供了安全保护。内部网络用户（位于 NAT 设备的内侧）连接互联网时，NAT 将用户的内部网络 IP 地址转换成一个外部公共 IP 地址（存储于 NAT 的地址池），并在 NAT 地址转换表中记录下这个转换项；当外部网络数据返回时，NAT 技术查询 NAT 地址转换表项，将目标 IP 地址替换成初始的内部用户的 IP 地址，把数据包转发给内部网络用户。由于这样对外隐藏了内部网络的 IP 地址，因此，外部用户无法直接发起到内部网络的连接，从而保护了内部网络用户。

一个有 NAT 能力的设备大多部署在存根网络的边缘，在图 20-2-1 中，R2 是边界路由器。如果 PC1、PC2 和 PC3 相互访问时，它们使用本来的私有 IP 地址；如果想访问外部主机时，数据包被转发给 R2，R2 执行 NAT 操作，把内部的私有地址转换成外部的、可路由的（私有地址本身也是可路由的，只是大多数 ISP 的路由器被配置成拒绝转发所有私有地址的流量）的公共 IP 地址后，再转发出去。

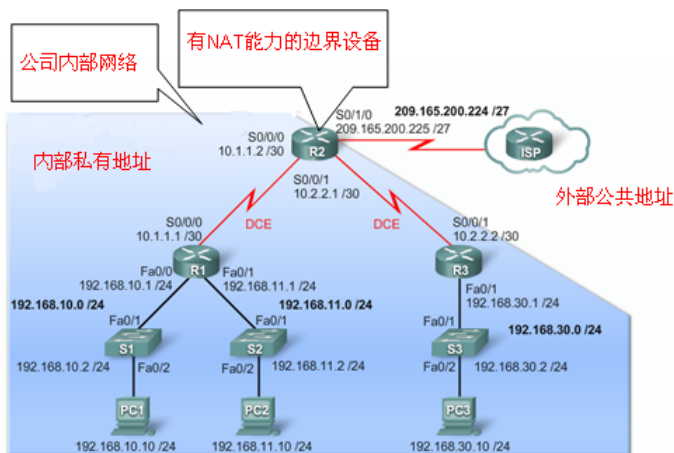


图 20-2-1 NAT 设备的部署位置

NAT 中的几个术语：

- **内部本地地址**（Inside local address）：分配给内部网络中计算机使用的 IP 地址。为了不和公共地址重叠，一般使用的都是私有地址。
- **内部合法地址**（Inside global address）：对外进行 IP 通信时，代表一个或多个内部本地地址的合法 IP 地址。需要申请才可取得的 IP 地址。
- **外部全局地址**（Outside global address）：分配给位于外部网络上的主机的 IP 地址，该地址是从全局可寻路径的地址或网络空间中分配的。
- **外部本地地址**（Outside local address）：在多数情况下，外部本地地址等于外部全局地址。



注意：外部本地地址的讨论超出 CCNA 的考试范围。

20.2.3 使用 NAT 的优点和缺点***

使用 NAT 有很多好处，然而使用 NAT 也带来一些不足，包括缺乏对一些流量的支持。

1. NAT 的优点

- NAT 节省了公共地址：一个企业申请的合法 IP 地址很少，而内部网络用户很多，可以通过 NAT 功能实现多个用户同时公用一个合法 IP 地址与外部网络进行通信。
- NAT 增加了连接到公网的弹性：可以使用多地址池、备份地址池、负载均衡地址池，确保可靠的公网连接。
- NAT 允许内部网络编址的一致性：如果一个单位没有使用私有地址和 NAT，当公有地址发生改变时，要改变公司内的所有主机的 IP 地址，工作量巨大。如果采用了 NAT，只更改 NAT 设备的 IP 地址池配置，内部网络的编址不受影响。这意味着，一个单位可以更换 ISP 而不需要改变内部主机的 IP 地址。
- NAT 提高了内部网络的安全：一个企业不想让外部网络用户知道自己内部网络的结构，可以通过 NAT 将内部网络与外部 Internet 隔离开，则外部用户根本不知道通过 NAT 设置的内部 IP 地址。NAT 虽然能提高内部网络的安全，但无法取代防火墙。

2. NAT 的缺点

- NAT 影响性能：转换每一个包头中的 IP 地址需要时间，NAT 增加了交换延时。路由器必须检查每一个包来决定是否需要转换，路由器需要转换 IP 头，有时还需要转换 TCP 或 UDP 头部。
- NAT 缺乏对一些应用的支持：很多 Internet 协议和应用依赖于端到端的应用，包从源到目的地不能被修改。通过修改端到端的地址，NAT 阻止了一些应用，比如一些安全应用，如数字签名就会失败，因为数据包中的源 IP 地址发生了改变。
- NAT 不利于追踪：经过多次 NAT，端到端的追踪变得非常困难。另外，因为 NAT 的存在，也很难追踪或获得黑客使用的真实 IP 地址。
- NAT 使一些隧道协议变得复杂：因为 NAT 修改了包头中的值，给 IPSec 或其他隧道协议的完整性检查带来困难。

20.2.4 配置静态 NAT**

NAT 设置可以分为静态地址转换、动态地址转换、复用动态地址转换。下面结合图 20-2-2 实现 3 种地址转换方式。在图 20-2-2 中，PC1 和 PC2 充当内网；真实计算机充当外网，真实计算机的网关为空（如果真实计算机的网关指向 218.1.1.1，不用配置 NAT，PC1 和 PC2 也可以访问真实计算机）；路由器 R1 充当 NAT 设备。

1. 静态地址转换适用的环境

静态地址转换将内部本地地址与内部合法地址进行一对一的转换，且需要指定和哪个合法地址进行转换。如果内部网络有 E-mail 服务器或 FTP 服务器等需要为外部用户提供服务，这些服务器的 IP 地址可以采用静态地址转换，以便外部用户可以使用这些服务。

2. 静态地址转换配置的基本步骤

- ① 指定连接外部网络的外部端口。在端口设置状态下输入：

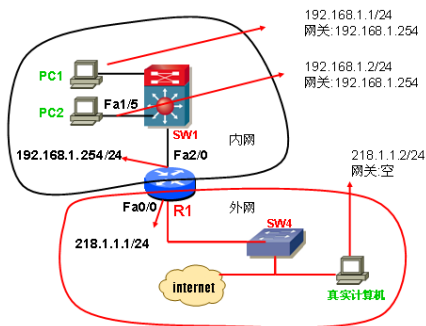


图 20-2-2 NAT 拓扑


```
ip nat outside
```

② 指定连接网络的内部端口。在端口设置状态下输入：

```
ip nat inside
```

③ 在内部本地地址与内部合法地址之间建立静态地址转换。在全局配置状态下输入：

```
ip nat inside source static 内部本地地址 内部合法地址
```

如果有多个 IP 地址需要静态地址转换，则需多次输入上述命令。

实验 20-4：配置静态 NAT

1. 配置 PC1、PC2

PC2 的配置略，PC1 的配置如下：

```
PC1(config)#int fa 0/0
PC1(config-if)#ip add 192.168.1.1 255.255.255.0
PC1(config-if)#no shut
PC1(config-if)#no ip routing
PC1(config)#no cdp run
PC1(config)#ip default-gateway 192.168.1.254
PC1(config)#ip http server
```

2. 配置路由器 R1

R1 配置如下（斜体部分是注释）：

（1）配置对外接口

```
R1(config)#int fa 0/0
R1(config-if)#ip add 218.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#ip nat outside      NAT 的对外接口。
```

（2）配置对内接口

```
R1(config-if)#int fa 2/0
R1(config-if)#ip add 192.168.1.254 255.255.255.0
R1(config-if)#no shut
R1(config-if)#ip nat inside      NAT 的对内接口。
R1(config-if)#exit
```

（3）配置转换条目

```
R1(config)#ip nat inside source static 192.168.1.1 218.1.1.10 配置 PC1 的转换条目。
R1(config)#ip nat inside source static 192.168.1.2 218.1.1.11 配置 PC2 的转换条目。
```

3. 测试

在 PC1 上 ping 真实计算机的 IP 地址 218.1.1.2，可以成功 ping 通。过程是这样的：

① PC1 发现要访问另一个网络的地址，PC1 把数据包发给网关 R1。

② R1 从 NAT 的 inside 接口收到一个数据包，R1 得知该数据包的目标地址是 218.1.1.2，R1 查询路由表，发现数据包要从 Fa0/0 端口发出去。该数据包满足 NAT 的执行条件，内部端口进来的包，要从外部端口发出去。R1 查找 NAT 地址转换表，发现有一个条目可以满足，R1 修改数据包的包头，把数据包中的源 IP 地址换成 218.1.1.10。R1 重新封装数据包，把数据链路层的源 MAC 地址更改成 Fa0/0 接口的 MAC 地址，把目的 MAC 地址更改成真实计算机的 MAC 地址，然后把数据报文转发出去。

③ 真实计算机收到这样的 ping 报文后，查看得知是来自 218.1.1.10 的报文。真实计算机进行应答，在数据包中封装的目的 IP 地址是 218.1.1.10，在数据帧中封装的目的 MAC 地

址是路由器 R1 Fa0/0 接口的 MAC 地址。真实计算机把数据报文发出。

④ R1 从 NAT 的外部接口收到一个数据报文，得知是发往本路由器的，且目的 IP 地址是 218.1.1.10，R1 查询 NAT 地址转换表，发现有一个静态的转换条目，R1 更改数据包中的目的 IP 地址，并重新封装后，把数据包发给 PC1。

至此，PC1 成功 ping 通真实计算机。如果在真实计算机上 ping 218.1.1.11，会出现什么情况呢？

因为真实计算机上没有 218.1.1.11 对应的 MAC 地址，真实计算机发送一个 ARP 查询包。R1 收到这个 ARP 查询包，R1 查询自己的 NAT 地址转换表，发现其中有 218.1.1.11 的转换条目，R1 用自己的 MAC 地址作应答。这里，R1 仅查询地址转换表就做出应答，并不关心这个 NAT 地址转换表中的源地址是否存在，这里在 R1 上再增加一个转换条目“ip nat inside source static 192.168.1.3 218.1.1.12”，并在真实计算机上 ping 218.1.1.12，R1 也会用自己的 MAC 地址应答，尽管 192.168.1.3 并不存在。

真实计算机收到 ARP 应答后，就知道了 218.1.1.11 对应的 MAC 地址，如图 20-2-3 所示。真实计算机封装数据包，发出 ping 的请求包。路由器 R1 收到这个数据报文，并转换 IP 头部，重新封装后发往 PC2，PC2 对 ping 请求报文进行应答。

真实计算机可以成功地 ping 通 218.1.1.11。如果在真实计算机上 ping 218.1.1.12 将失败，是因为 192.168.1.3 并不存在。

在真实计算机 IE 浏览器的地址栏中输入 http://218.1.1.10，可以成功访问到 PC1 的 Web 页面，如图 20-2-4 所示。

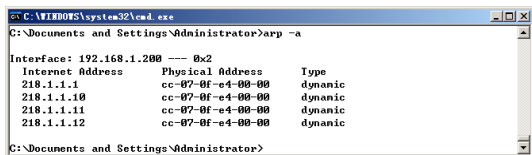


图 20-2-3 查看真实计算机的 ARP 缓存

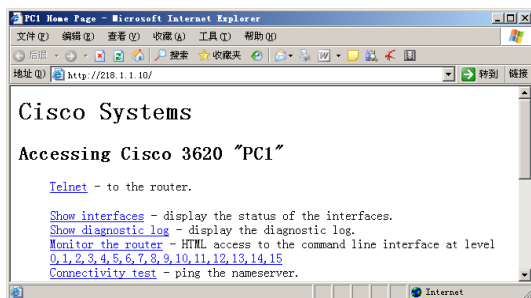


图 20-2-4 访问静态 NAT 的内网

20.2.5 配置动态 NAT**

1. 动态地址转换适用的环境

动态地址转换也是将内部本地地址与内部合法地址进行一对一的转换，但是动态地址转换是从内部合法地址池中动态地选择一个没有使用的合法地址对内部本地地址进行转换。

2. 动态地址转换的基本配置步骤

① 指定与外部网络相连的外部端口，在端口设置状态下输入：

```
ip nat outside
```

② 指定与内部网络相连的内部端口，在端口设置状态下输入：

```
ip nat inside
```

③ 在全局配置模式下，定义内部合法地址池：

```
ip nat pool 地址池名称 起始 IP 地址 终止 IP 地址 子网掩码
```

④ 在全局配置模式下，定义一个 **access-list** 规则以允许哪些内部地址可以进行动态地址转换：

```
Access-list 表号 permit 源地址 通配符
```

其中，表号为 1~99 之间的整数，是标准访问控制列表。也可以使用扩展访问控制列表，表号为 100~199，以实现更复杂的地址转换限制。

⑤ 在全局配置模式下，将由 **access-list** 指定的内部本地地址与指定的内部合法地址池进行地址转换：

```
ip nat inside source list 访问列表标号 pool 内部合法地址池名字
```

使用动态地址转换方式，在图 20-2-2 中，R1 的配置如下：

(1) 配置对外接口

```
R1(config)#int fa 0/0
R1(config-if)#ip add 218.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#ip nat outside          NAT 的对外接口。
```

(2) 配置对内接口

```
R1(config-if)#int fa 2/0
R1(config-if)#ip add 192.168.1.254 255.255.255.0
R1(config-if)#no shut
R1(config-if)#ip nat inside          NAT 的对内接口。
R1(config-if)#exit
```

(3) 配置地址池

```
R1(config)#ip nat pool pool1 218.1.1.10 218.1.1.20 netmask 255.255.255.0
```

(4) 配置允许被转换的地址列表

```
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

(5) 把允许被转换的地址列表和地址池对应起来

```
R1(config)#ip nat inside source list 1 pool pool1
```

3. 动态 NAT 和静态 NAT 的比较

动态 NAT 和静态 NAT 一样，使用的都是一对一转换，但二者还是有区别的，主要体现在以下几点：

- 动态 NAT 允许内网有超过地址池中 IP 地址的数量的用户被转换，但同时被转换出去的用户数不能超过地址池中的 IP 地址的数量。静态 NAT 有多少个 IP 地址，就只能配置多少个转换。
- 动态 NAT 中刚开始是没有 NAT 转换条目的，只有内网用户访问外网时，才会动态创建转换条目。静态 NAT 中的条目是一直存在的。
- 在动态 NAT 中，外网不确定连接哪一个公网地址才能访问到内网主机，因为转换是动态的，静态 NAT 中转换条目是固定的。

4. 测试

① 在路由器 R1 上，执行“show ip nat translations”命令，可以发现没有任何转换条目存在，如图 20-2-6 中上面的那条命令的执行结果。

② 在真实计算机上执行“ping 218.1.1.10”命令，收不到应答；执行“arp -a”命令显示 ARP 缓存，缓存中没有条目 218.1.1.10，如图 20-2-5 所示。

③ 在 PC1 上 ping 真实计算机的 IP 地址“218.1.1.2”，发现可以成功 ping 通。

④ 再次在 R1 上执行“show ip nat translations”命令，如图 20-2-6 中下面那条命令的执行结果。

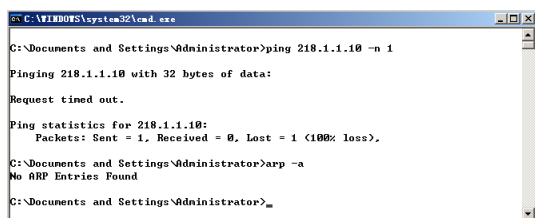


图 20-2-5 动态 NAT 转换前的测试

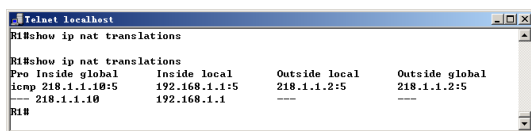


图 20-2-6 查看转换条目

可以看到 PC1 发起访问外网后，触发了地址转换功能，192.168.1.1 被转换成了 218.1.1.10，因为是 ping，还触发了一个 ICMP 的转换。可以使用“clear ip nat translation *”命令清除所有的转换条目，使用“show ip nat translations verbose”命令查看 NAT 转换的详细信息，如图 20-2-7 所示。从图中可以看出 ICMP 转换条目的超时时间默认是 1 分钟，已经过去 7 秒，还剩 52 秒；IP 地址转换条目的默认超时时间是 24 小时。

⑤ 再次在真实计算机上执行“ping 218.1.1.10”命令，收到应答；执行“arp -a”命令显示 ARP 缓存，缓存中有条目 218.1.1.10，如图 20-2-8 所示。

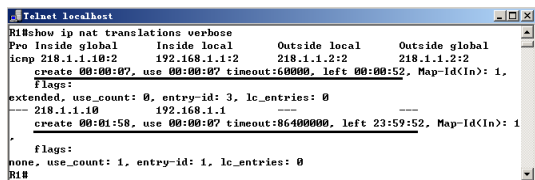


图 20-2-7 查看 NAT 的详细情况

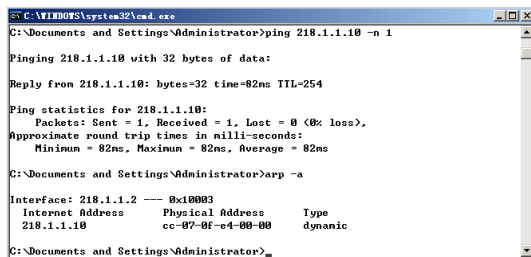


图 20-2-8 动态 NAT 转换后的测试

20.2.6 配置 NAT 超载***

NAT 超载也称复用动态地址转换。

1. 复用动态地址转换适用的环境

这是现实中使用最多的一种地址转换方式，有时也称 PAT (Port Address Translation，端口地址转换)。复用动态地址转换首先是一种动态地址转换，但是它可以允许多个内部本地地址共用一个内部合法地址。只申请到少量 IP 地址，但却经常同时有多于合法地址个数的用户访问外部网络的情况，这种转换极为有用。PAT 采用的工作原理是：当多个用户同时使用一个 IP 地址时，路由器利用上层的 TCP 或 UDP 端口号等唯一标识某台计算机。

2. 复用动态地址转换的配置步骤

复用动态地址转换的配置步骤与动态地址转换的配置步骤几乎完全相同，仅在配置内

部本地地址与内部合法 IP 地址池对应时，多加一个参数 “overload”。

20.2.7 配置端口映射**

仅有一个本地合法地址，要实现内部所有主机共享上网，可以通过配置 NAT 超载实现。如果单位内部还要对外网提供 WWW、E-mail 等服务，此时还需要增加配置端口映射。在配置 NAT 超载的基础上，增加端口映射的配置。比如，配置路由器 R1，使外网对 IP 地址 218.1.1.1 的 TCP 80 端口的访问转换成对内部本地 IP 地址 192.168.1.1 的 80 端口的访问。配置端口映射的命令是 “R1(config)#ip nat inside source static tcp 192.168.1.1 80 218.1.1.1 80”。

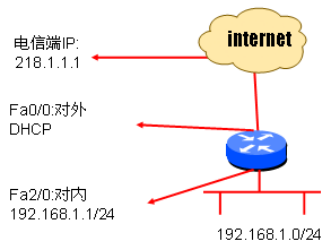


图 20-2-9 电信动态宽带接入

实验 20-5：电信动态宽带接入中 NAT 的配置

电信宽带接入的方式有静态接入和动态接入两种。静态接入就是提供固定的 IP 地址，方便被接入单位对公网提供服务，价格相对较贵。动态接入不提供固定的 IP 地址，被接入单位通过 DHCP 获取地址，如图 20-2-9 所示。针对动态接入方式，复用动态地址转换的配置如下（斜体部分是注释）：

```
Router(config)#int fa 0/0
Router(config-if)#ip add dhcp
Router(config-if)#ip nat outside
Router(config-if)#no shut
Router(config-if)#int fa 2/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat inside source list 1 int fa 0/0 overload
不用创建地址池，直接借用 Fa0/0 的 IP 地址，Fa0/0 获取什么地址就使用什么地址。这样配置 NAT 超载的 5
个步骤就变成 4 个步骤了。该方法同样适用于静态接入。
Router(config)#ip route 0.0.0.0 0.0.0.0 218.1.1.1 配置默认路由。
```



20.3 真题精选***

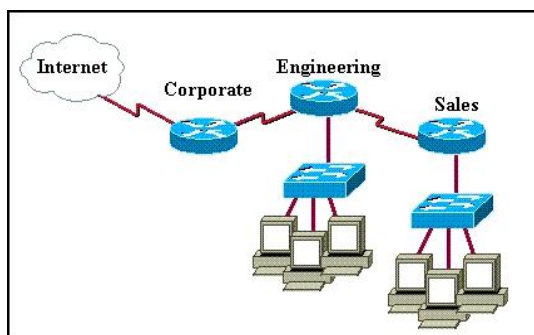
- How does a DHCP server dynamically assign IP addresses to hosts?
 - Addresses are permanently assigned so that the host uses the same address at all times.
 - Addresses are assigned for a fixed period of time. At the end of the period, a new request for an address must be made, and another address is then assigned.
 - Addresses are leased to hosts. A host will usually keep the same address by periodically contacting the DHCP server to renew the lease.
 - Addresses are allocated after a negotiation between the server and the host to determine the length of the agreement.
- What TCP/IP stack configuration features can DHCP provide, in addition to assigning an IP address? (Choose three.)

A. default gateway	B. DNS servers
C. FTP server	D. helper address
E. subnet mask	F. TFTP server

3. Which of the following describe private IP addresses? (Choose two.)

- A. addresses chosen by a company to communicate with the Internet
- B. addresses that cannot be routed through the public Internet
- C. addresses that can be routed through the public Internet
- D. a scheme to conserve public addresses
- E. addresses licensed to enterprises or ISPs by an Internet registry organization

4. A network administrator would like to implement NAT in the network shown in the graphic to allow inside hosts to use a private addressing scheme. Where should NAT be configured?



- A. Corporate router
- B. Engineering router
- C. Sales router
- D. all routers
- E. all routers and switches

5. What does the "Inside Global" address represent in the configuration of NAT?

- A. the summarized address for all of the internal subnetted addresses
- B. the MAC address of the router used by inside hosts to connect to the Internet
- C. a globally unique, private IP address assigned to a host on the inside network
- D. a registered address that represents an inside host to an outside network

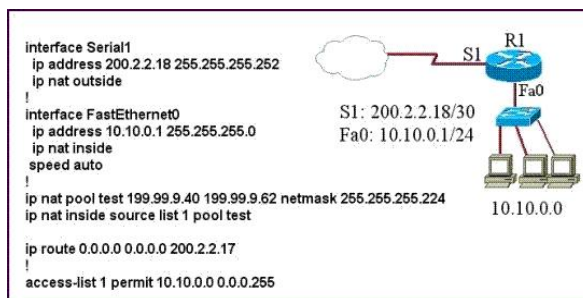
6. What is the function of the Cisco IOS command `ip nat inside source static`

10.1.1.5 172.35.16.5?

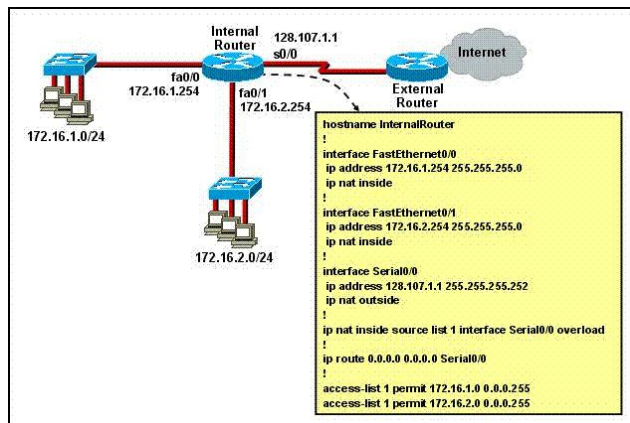
- A. It creates a global address pool for all outside NAT transactions.
- B. It establishes a dynamic address pool for an inside static address.
- C. It creates dynamic source translations for all inside local PAT transactions.
- D. It creates a one-to-one mapping between an inside local address and an inside global address.
- E. It maps one inside source address to a range of outside global addresses.

7. Refer to the topology and router configuration shown in the graphic. A host on the LAN is accessing an FTP server across the Internet. Which of the following addresses could appear as a source address for the packets forwarded by the router to the destination server?

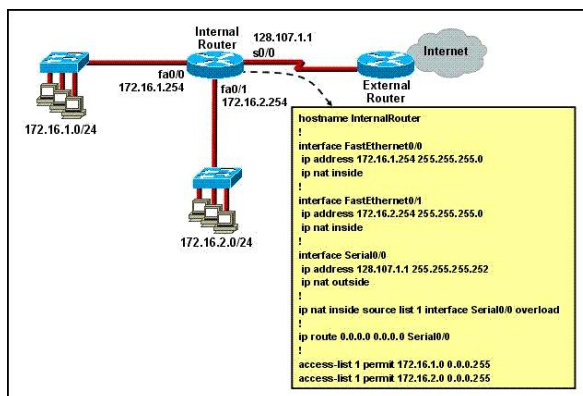
- A. 10.10.0.1
- B. 10.10.0.2
- C. 199.99.9.33
- D. 199.99.9.57
- E. 200.2.2.17
- F. 200.2.2.18



8. Refer to the exhibit. What is the purpose of the configuration that is shown?



- to translate addresses of hosts on the fa0/0 and fa0/1 networks to a single public IP address for Internet access
 - to translate the internal address of each host on fa0/0 and fa0/1 to a unique external IP address for Internet access
 - to provide security on fa0/0 and fa0/1 through the application of an access list
 - to allow IP hosts on the Internet to initiate TCP/IP connections to hosts on fa0/0 and fa0/1
9. Refer to the exhibit. What statement is true of the configuration for this network?



- The configuration that is shown provides inadequate outside address space for translation of the number of inside addresses that are supported.

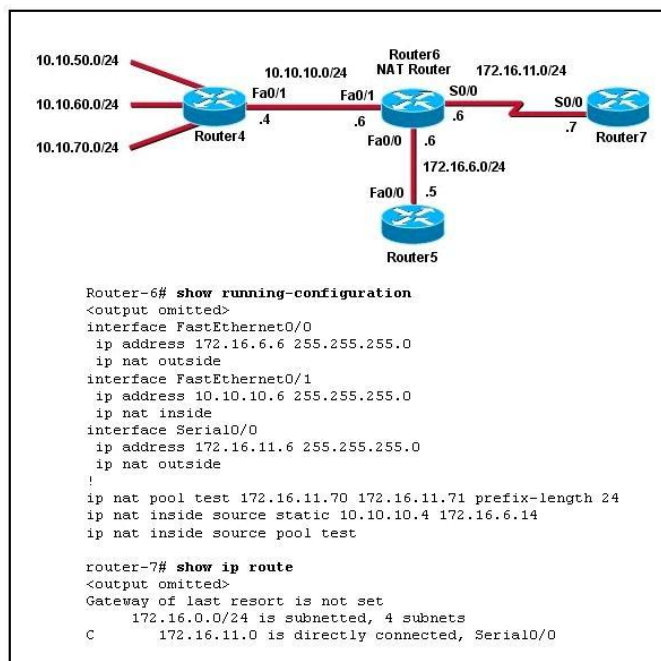
- B. Because of the addressing on interface FastEthernet0/1, the Serial0/0 interface address will not support the NAT configuration as shown.
- C. The number 1 referred to in the ip nat inside source command references access-list number 1.
- D. External Router must be configured with static routes to networks 172.16.1.0/24 and 172.16.2.0/24.

10. Refer to the output from the show running-config command in the exhibit. What should the administrator do to allow the workstations connected to the FastEthernet 0/0 interface to obtain an IP address?

- A. Apply access-group 14 to interface FastEthernet 0/0.
- B. Add access-list 14 permit any any to the access list configuration.
- C. Configure the IP address of the FastEthernet 0/0 interface to 10.90.201.1.
- D. Add an interface description to the FastEthernet 0/0 interface configuration.

```
R1-ABC# show running-config
Current configuration:
!
version 12.1
hostname ABC
!
ip subnet-zero
ip name-server 192.16.1.1
ip dhcp excluded-address 10.90.201.1
!
ip dhcp pool ABC_DHCP
network 10.90.201.0 255.255.255.0
default-router 10.90.201.1
dns-server 192.31.7.152
!
interface FastEthernet 0/0
no ip directed-broadcast
ip nat inside
!
interface Serial 0/0
description to ISP circuit ID ALDS1-3456AX4743-00
ip address 192.31.7.38 255.255.255.252
ip nat outside
!
ip nat inside source list 14 interface serial 0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 192.31.7.37
!
access-list 14 permit 10.90.201.0 0.0.0.255
<output omitted>
```

11. Refer to the exhibit. Router4 can ping Router5 (172.16.6.5), but not Router7 (172.16.11.7). There are no routing protocols running in any of the routers, and Router4 has Router6 as its default gateway. What can be done to address this problem?



- A. Convert to static NAT.
- B. Convert to dynamic NAT.

- C. Add a static route in Router7 back to Router4.
- D. Change the inside and outside NAT commands.



20.4 真题解答***

1. 解: C

题目问: 一台 DHCP 服务器是怎样动态分配一个 IP 地址给主机的? A 选项说地址被永久地分配, 因此主机在任何时间使用的都是相同的地址。B 选项说地址被分配一个固定的租期, 在租期结束后, 一个新的 DHCP 请求被发出, 然后被分配另一个地址。C 选项说地址被主机租用, 一台主机周期性地与 DHCP 联系来更新租期, 主机将经常保持同一个地址。D 选项说在服务器和主机之间协商使用被分配地址的使用期限。DHCP 是一个动态主机分配协议, 与 BOOTP 不同, BOOTP 是静态地永久分配。DHCP 是动态地分配 IP 地址, 并提供租约, 在租约过去一半时, 客户端会与服务器进行联系, 以更新租约, 更新租约后, 获取的 IP 地址不变, 使用的期限被延长。如果多次联系失败, 客户机将在租期到达时, 释放获取的 IP 地址。根据 DHCP 协议的特点, 只有 C 选项是正确的。

2. 解: ABE

题目问: 在 TCP/IP 协议栈中, DHCP 除了分配 IP 地址外, 还用来提供什么 (选 3 个)? 正确的答案应该选择: 子网掩码、网关、DNS 服务器。故 A、B 和 E 正确。

3. 解: BD

题目问: 下面哪一个描述了私有 IP 地址 (选 2 个)? A 选项说是公司用来和 Internet 通信的地址, 能和 Internet 通信的是公共地址而不是私有地址。B 选项说不能被公网路由的地址, Internet 中的所有路由器都不转发去往私有网段的数据包。B 正确, 则 C 错误。D 选项说是一种节省公共地址的方案, 使用 NAT 最主要的目的就是节省公共地址, 仅通过少量的公共地址, 可以使用更多的主机访问 Internet。E 选项说被 ISP 或 Internet 注册机构授权给企业的, 这也是公共地址。故正确答案是 B 和 D。

4. 解: A

题目问: 参照图, 网络管理员将配置 NAT 来允许内部主机使用私有地址, NAT 配置在哪里比较合适? 参照图 20-2-1, NAT 应配置在公司的边界路由器上, 而不是内部路由器上。所以正确答案选 A。

5. 解: D

题目问: 在配置 NAT 时, “Inside Global” 代表什么? Inside Global 是内部全局地址, 是经过注册的、合法的、可以和外部通信的地址。A 选项说是内部所有子网地址的汇总地址。B 选项说是 MAC 地址。C 选项前面说是一个全局唯一的地址, 是正确的, 后面说是一个私有的 IP 地址, 可以分配给内网的主机使用的说法是错误的。D 选项说是一个被注册的地址, 用来对外部网络表示内部主机, 这种说法是正确的。

6. 解: D

题目问: “ip nat inside source static 10.1.1.5 172.35.16.5” 这句 IOS 命令的作用是什么? 本题考的是 NAT 静态地址转换, 这条命令的作用是静态地创建一个一对一的地址转换,

把内部本地地址 10.1.1.5 转换为内部全局地址 172.35.16.5。故选 D。

7. 解: D

题目问: 参照图, 局域网中的一台主机访问 Internet 上的 FTP 服务器, 路由器把包发往目的服务器, 选项中的哪一个 IP 地址能出现在包的源地址中? 本题考的是 NAT 动态地址转换, Fa0 接口连接的是私有地址, 这些地址是不能同外网进行通信的, 这时就需要借助 NAT, 将内网的私有地址转换为可以在公网上通信的地址。我们看到 NAT pool 中定义的转换后的公有地址为 199.99.9.40 到 199.99.9.62, 则表示这段地址是转换后的内网全局地址, 所以内网主机想要穿过 Internet 访问 FTP 服务器, 则需要转换为 199.99.9.40 到 199.99.9.62 之内的公有地址。在上面的答案中只有地址 199.99.9.57 满足条件, 所以答案选 D。

8. 解: A

题目问: 图中配置的目的是什么? 从图中可以看出这是 NAT 超载的配置, 其中 fa0/0 和 fa0/1 是对内接口, s0/0 是对外接口, 没有配置内部合法地址池, 所有内网用户借助 s0/0 接口的 IP 地址访问外网。B 选项说在 fa0/0 和 fa0/1 接口的每一台主机都使用一个唯一的 IP 地址访问 Internet, 其实两个接口连接的所有主机都使用 s0/0 接口的一个 IP 地址 128.107.1.1 访问 Internet。C 选项说通过访问控制列表实现安全, 是错误的。D 选项说允许 Internet 发起对 fa0/0 和 fa0/1 接口主机的连接, 也是错误的。

9. 解: C

题目问: 参照图中的配置, 哪一个语句是正确的? A 选项说这个显示的配置没有为内部所有主机提供充分的外部转换地址, 本配置使用的是 NAT 超载技术, s0/0 的一个 IP 地址可以提供内部很多主机同时访问 Internet, 外部 IP 地址是够用的。B 选项说因为 FastEthernet0/1 接口的 IP 地址, Serial0/0 接口将不支持列出的配置, 图中列出的配置是可以支持的。C 选项说 “ip nat inside source list 1” 中的 1 参照 access-list 1, 这个说法是正确的。D 选项说外部路由器必须要配置到 172.16.1.0/24 和 172.16.2.0/24 的静态路由, 外部路由器看到的地址是 128.107.1.1, 根本不需要配置到内部私有地址的路由。故正确答案是 C。

10. 解: C

题目问: 参照图中 “show running-config” 命令的输出, 网络管理员将做什么允许连接到 FastEthernet 0/0 接口的工作站获得 IP 地址? 从图中的配置可以看出, FastEthernet 0/0 接口是对内接口, 是内部工作站的网关, 可是该接口没有配置 IP 地址。从 DHCP 地址池的配置中可以看出, 这里分配的 default-router 是 10.90.201.1, 从上面的分析中, 可以看出 C 是正确答案。

11. 解: C

题目问: 参照图, 任何路由器上都没有配置路由协议, Router4 把 Router6 作为默认网关, Router4 能够 ping 通 Router5 (172.16.6.5), 但却 ping 不通 Router7 (172.16.11.7)。做什么来解决这个问题? 这个题的难度非常大, 题目同时涉及静态 NAT 和动态 NAT。静态 NAT 使路由 Router4 不管是 ping 路由器 Router5, 还是 ping 路由器 Router7, 都被转换成 172.16.6.14 这个 IP 地址, 所以 ping 路由器 Router5 是成功的; 但 ping 路由器 Router7 时, Router6 把数据包转发到 Router7, 但 Router7 上没有去往 IP 地址 172.16.6.14 的路由, 所以

ping 失败。题目的配置中试图再配置一个动态 NAT 来实现 Router4 ping 路由器 Router7，这种做法是不正确的，有静态 NAT 的话，就使用不到动态 NAT 了，而且题中动态 NAT 配置还有错误，在显示的配置中，“ip nat inside source pool test”这句是错误的，里面少了一个关键字 list，就算有 list，还缺少对应的 access-list。就算把动态 NAT 配置正确也无法使 Router4 ping 通 Router7。A 选项说转换静态 NAT，静态 NAT 配置是正确的，就算修改也是达不到要求的。B 选项说转换动态 NAT，就算配置正确也是无法达到要求的。C 选项说在 Router7 添加一条回 Router4 的静态路由，更准确地说应该是添加一条回 172.16.6.14 的路由，如果追求完美，还需要删除“ip nat pool test...”和“ip nat inside source pool test”两句多余的配置。D 选项说更改对内对外端口也是难以实现的。故 C 选项正确。

第 21 章

IPv6***

本章主要介绍 IPv6 的重要性、IPv6 的地址表示格式、IPv6 的静态和动态路由配置，以及从 IPv4 向 IPv6 过渡阶段二者共存的一些实现技术。本章是 CCNA 640-802 考试大纲中新增加的内容，考题多是理论性的。掌握一些 IPv6 的技术更能让您在未来的 IPv6 普及中获得先机。



21.1 IPv6 的重要性***

显然，IPv6 的优势能够对上述挑战直接或间接地做出贡献。其中最突出的是 IPv6 大大地扩大了地址空间，恢复了原来因地址受限而失去的端到端连接功能，为互联网的普及与深化发展提供了基本条件。当然，IPv6 并非十全十美、一劳永逸，不可能解决所有问题。IPv6 只能在发展中不断完善，也不可能在一夜之间发生，过渡需要时间和成本，但从长远看，IPv6 有利于互联网的持续和长久发展。

目前，Internet 中广泛使用的是 IPv4 协议，也就是人们常说的 IP 协议。随着 Internet 技术的迅猛发展和规模的不断扩大，IPv4 已经暴露出了许多问题，而其中最重要的一个问题就是 IP 地址资源的短缺。造成 IP 地址短缺的原因主要有：

- 上网人数的增加（Population growth）：起初 Internet 的使用者主要是大学、高新技术产业工业，以及政府部门，随着 20 世纪 90 年代中期 Internet 的不断膨胀，它已被更多的人使用，尤其是有着不同需求的人们。
- 移动用户（Mobile users）：越来越多的具有 IP 功能的移动设备接入互联网，包括个人数字助理（PDA）、笔记本电脑等。
- 交通运输（Transportation）：到 2008 年有超过 10 亿的汽车是启用 IP 功能的，可以提供远程监控和及时的维护与支持。
- 电子设备（Consumer electronics）：可能不久的将来世界上的每一台家电都会成为 Internet 的一个结点。

为了彻底解决 IPv4 存在的问题，IETF 从 1995 年开始就着手研究开发下一代 IP 协议，即 IPv6。IPv6 具有长达 128 位的地址空间，允许有 2^{128} (约 3.4×10^{38}) 个地址，可以彻底解决 IPv4 地址不足的问题，据估计地球每平方米大约可以分配 665 570 793 348 866 943 898 599 个 IP 地址，除此之外，IPv6 还采用了分级地址模式、高效 IP 包头、服务质量、主机地址自动配置、认证和加密等许多技术。IPv6 与 IPv4 相比，有以下优势：

(1) Enhanced IP addressing（增强的 IP 地址）

- Global reachability and flexibility（全局可达性和灵活性），这是因为没有使用 NAT

技术;

- Aggregation (聚合), IPv6 地址全球分配更合理, 更容易汇聚;
- Multihoming (多宿主), 一台设备可以有多个网络号;
- Autoconfiguration (自动配置), 网络中的设备可以自动配置地址;
- Plug-and-play (即插即用);
- End-to-end without NAT (没使用 NAT 也可端到端);
- Renumbering (重新编址), 重新分配地址很方便。

(2) Mobility and security (移动和安全)

- Mobile IP RFC-compliant (与 RFC 兼容的移动 IP);
- IPsec mandatory (or native) for IPv6 (IP 的安全被强制执行)。

(3) Simple header (简单的包头), IPv6 比 IPv4 的包头更简单

- Routing efficiency (路由更高效);
- Performance and forwarding rate scalability (性能和转发速率可预测);
- No broadcasts (没有广播), IPv6 和 IPv4 不同, IPv6 中没有广播;
- No checksums (没有检验和);
- Extension headers (扩展头部);
- Flow labels (流标签)。

从 IPv4 到 IPv6 的转换涉及大量的设备需要升级, 太多的技术人员需要培训, 不是一朝一夕可以完成的, 有下面几种技术可以支持 IPv4 和 IPv6 的共存。

- Dual-stack (双栈);
- 6to4 and manual tunnels (IPv6 到 IPv4 和手动隧道);
- Translation (地址转换)。

现在已经是 2010 年, 可是 IPv6 并没有像当初预想的那样迅速取代 IPv4, 很大一部分原因在于 NAT 技术的成功运用。但请坚信 IPv6 终有一天会在全球实现。



21.2 IPv6 地址***

本节介绍 IPv6 的地址表示、IPv6 的地址类型、IPv6 的地址分配。

21.2.1 IPv6 地址表示***

IPv6 的 128 位地址是以 16 位为一分组, 每个 16 位分组写成 4 个十六进制数, 中间用冒号分隔, IPv6 地址中不区分字母的大小写, 称为冒号分十六进制数格式。

例如: 2031:0000:130F:0000:0000:09C0:876A:130B 是一个完整的 IPv6 地址。

IPv6 真是难以记忆和书写, 但有以下几种可以简化的特殊情形:

- IPv6 地址中每个 16 位分组中的前导零位可以去除做简化表示, 但每个分组必须至少保留一位字符。比如上例中的地址, 去除前导零位后可写成: 2031:0:130F:0:0:9C0:876A:130B。
- 某些地址中可能包含很长的零序列, 为进一步简化表示法, 还可以将冒号分十六进制数格式中相邻的连续零位合并, 用双冒号 "::" 表示。“::” 符号在一个地址中只能出现一次, 该符号也能用来压缩地址中前部和尾部相邻的连续零位。例如地址 2031:0000:130F:0000:0000:09C0:876A:130B、0:0:0:0:0:0:1、0:0:0:0:0:0:0 分别可表

示成 2031:0:130F::9C0:876A:130B、::1、::。

21.2.2 IPv6 地址类型***

IPv6 中的地址有单播地址（Unicast）、组播地址（Multicast）和任意播地址（Anycast），当然还包含一些特殊的地址类型，接下来简单讨论这些地址。

1. 全局单播地址

全局单播地址可以分配给任何一个想接入互联网的用户或者分配给任何一个希望被全球可路由的设备。IANA 组织当前划定的全局单播地址是 2000::/3，占整个 IPv6 地址空间的 1/8，然后 IANA 再把这个地址空间逐级分下去。如图 21-2-1 所示，/23 是注册机构前缀，/32 是 ISP 运营商前缀，/48 是站点前缀，/64 是子网前缀，这样划分结构清晰，很容易进行汇聚。

单播地址和任意播地址都来自全局单播地址空间。记住：IPv6 中没有广播地址。

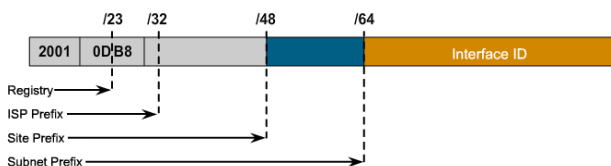


图 21-2-1 IPv6 的地址分配

2. 组播地址

IPv6 组播地址和 IPv4 组播地址的作用相同。前 8 个比特是 FF。接下来的 4 比特是地址的生存期；0 是永久，1 是临时，从 2~F 都保留没有使用。再接下来的 4 比特说明了组播地址的范围，也就是可以到达多远：1 表示节点，2 表示链路，5 表示站点，8 表示组织，E 表示整个因特网。譬如以 FF02::/16 开头的组播地址表示的是一个永久性的链路组播地址。

3. 保留地址

IPv6 的地址被保留了部分留给现在或将来使用。

4. 任意播地址

IPv4 中使用了广播，网段上的每台设备都必须处理广播。在 IPv6 中，没有广播地址类型，被组播地址代替。任意播地址来自全局单播地址空间，一组接口（一般属于不同节点）可以被分配相同的任意播地址。任意播是单播和组播的混合体。就单播来说，一个分组送到一个接收站；就组播来说，一个分组被送到组播中的所有成员；而对任意播来说，一个分组被转发到被配置任意播地址的接口之一（路由协议度量值最小的），有时任意播地址也被称为 one-to-nearest 地址。读者可以这样来理解任意播地址，譬如电信在全国有多台路由器，都配置了相同的 IPv6 地址（也就是任意播地址），但不同地区的请求都被路由到离该地区最近的电信路由器上，可以起到负载分担的作用。IPv6 任意播地址存在下列限制：

任意播地址不能用做源地址，而只能作为目的地址；

任意播地址不能指定给 IPv6 主机，只能指定给 IPv6 路由器。

注意：路由器同一个接口可以被配置多个 IPv6 地址，而不需要使用 Secondary 参数。此外路由器同一个接口也可以同时配置多种 IPv6 地址类型，譬如全局单播和任意播地址。

5. 私有地址

IPv6 的私有地址和 IPv4 的私有地址差不多，都是在本地有意义，前两个字符是 FE，第三个字符从 8 到 F。IPv6 的私有地址有两种：Site-local addresses（站点本地地址）和 Link-local addresses（链路本地地址），它们各有特殊的意义。

（1）**链路本地地址**：链路本地地址也是一种 IPv6 独有的地址，当两个支持 IPv6 特性的路由器直连时，直连的接口会自动给自己分配一个链路本地地址，其主要作用是在没有管理员的配置下设备间就能够相互通信，并且完成邻居发现等工作。链路本地地址前 3 个字符可以是：FE8、FE9、FEA、FEB。常见的链路本地地址以 FE80/10 打头，接下来的 54bit 全 0，最后 64bit 是 EUI-64 地址，有关 EUI-64 地址稍后介绍。

（2）**站点本地地址**：站点本地地址和链路本地地址一样，站点本地地址也是 IPv6 独有的 IP 地址，但区别在于链路本地地址只能用于共享链路上的设备，而站点本地地址可以用于站点内部，获得站点本地地址的设备是不能将数据包路由到站点之外的，也就是说，站点本地地址将限制数据包的传递。站点本地地址前 3 个字符可以是：FEC、FED、FEE、FEF。

6. 环回地址

IPv4 中以 127 打头的 IP 地址都是环回地址，而在 IPv6 中只有一个 IP 地址是环回地址，那就是 0:0:0:0:0:0:0:1，即“::1”。

7. 不确定地址

IPv4 中不确定地址是用 0.0.0.0 表示的，IPv6 中用 0:0:0:0:0:0:0:0 表示，即“::”。

21.2.3 配置 IPv6 地址*

IPv6 的地址可能被静态配置或动态配置，配置的方法有：

1. 手工静态配置

在思科路由器上，可以在接口下使用“`ipv6 address ipv6-address/prefix-length`”命令配置。比如给路由器 Fa0/0 接口配置 IPv6 地址 2001:DB8:2222:7272::72/64，则可以通过下面的命令完成：

```
Router(config-if)#ipv6 address 2001:DB8:2222:7272::72/64
```

2. 静态 EUI-64 配置

EUI-64（Extended Unique Identifier 64，扩展唯一标识符 64）是扩展 MAC 地址，由 64 位组成，通过在 MAC 地址的中间，也就是第 24 位的前面插入 16 位 0xFFFE，以创建一个 64 位，独特的接口标识符。在思科路由器上，可以在接口下使用“`ipv6 address ipv6-prefix/prefix-length eui-64`”命令配置，比如给路由器 Fa0/0 接口配置前缀是 2001:DB8:2222:7272::/64 的 EUI-64 格式的 IPv6 地址，则可以通过下面的命令完成：

```
Router(config-if)#ipv6 address 2001:DB8:2222:7272::/64 eui-64
```

假如路由器的 MAC 地址是 0090:27FF:FE17:FC0F，则 EUI-64 的值是 0090:27FF:FE17:FC0F，如图 21-2-2 所示。路由器 Fa0/0 接口的 EUI-64 格式的 IPv6 地址是：2001:DB8:2222:7272:0090:27FF:FE17:FC0F/64。

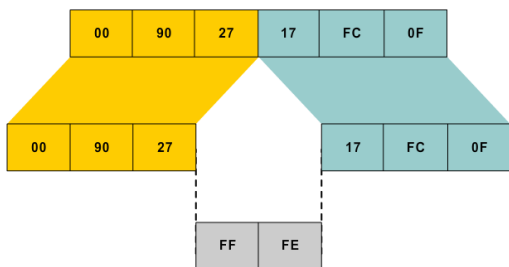


图 21-2-2 EUI-64 计算

3. 无状态自动配置

在 IPv6 中，一些电脑以及非电脑设备连接到网络，客户端通过获得路由器通告源地址的前 64 位，并使用 EUI-64 被充后 64 位，完成 IPv6 地址的配置。这种自动配置方式可以使联网的这些设备自动获得 IP 地址，实现即插即用，帮助减少管理员的负担。

4. DHCPv6

该功能与 IPv4 的 DHCP 功能类似。



21.3 IPv6 路由*

像 IPv4 的无类域间路由（CIDR）一样，IPv6 使用的也是最长前缀匹配原则。本节讲述 IPv6 的静态路由和动态路由配置。

IPv6 的地址分配如图 21-3-1 所示，分别配置静态路由和动态路由，保证网络的连通性。正式开始配置前请先更换 R2 的 IOS 版本，因为 R2 的 IOS 是支持高级安全特性的版本，不支持 IPv6 功能。用记事本打开模拟器文件夹中的“labini\ccna.net”，找到如下内容：

```
[[router R2]]
image = ..\IOS\unzip-c7200-advsecurityk9-mz.124-9.T1.bin
```

把“unzip-c7200-advsecurityk9-mz.124-9.T1.bin”更换成“unzip-c7200-js-mz.123-20.bin”，并保存修改。

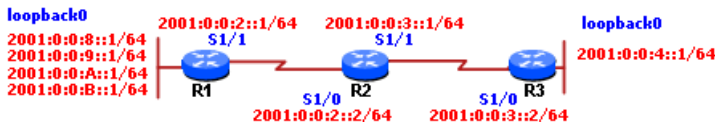


图 21-3-1 配置 IPv6 路由

1. 静态路由的配置

IPv6 的静态路由工作原理与 IPv4 相同，这里不再多叙。实验 21-1 列出了每台设备的配置和解释。

实验 21-1：配置 IPv6 静态路由

R1 的配置如下（斜体部分是注释）：

```
Router>en
Router#conf t
Router(config)#host R1
```

```
R1(config)#ipv6 unicast-routing 路由器默认不支持 IPv6 路由，需要该命令全局开启。
R1(config)#int s1/1
R1(config-if)#ipv6 address 2001:0:0:2::1/64 配置 IPv6 地址。
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ipv6 address 2001:0:0:8::1/64 配置 IPv6 地址。
R1(config-if)#ipv6 address 2001:0:0:9::1/64
配置第二个 IPv6 地址，IPv6 中一个接口下可以配置多个地址，输入的命令格式不变，也不像 IPv4 中需要加 Secondary。
R1(config-if)#ipv6 address 2001:0:0:10::1/64
R1(config-if)#ipv6 address 2001:0:0:11::1/64
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#ipv6 route ::0 2001:0:0:2::2
和 IPv4 中配置静态路由有些差异，IPv4 中是网络号后跟网络掩码，IPv6 中是网络号后跟“/网络前缀长度”。这里配置的是默认路由，::0 相当于 0:0:0:0:0:0:0:0。
```

R2 的配置如下（斜体部分是注释）：

```
Router>
Router>en
Router#conf t
Router(config)#host R2
R2(config)#ipv6 unicast-routing
R2(config)#int s1/0
R2(config-if)#ipv6 address 2001:0:0:2::2/64
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ipv6 address 2001:0:0:3::1/64
R2(config-if)#no shut
R2(config)#ipv6 route 2001:0:0:8::/62 2001:0:0:2::1
去往 R1 环回接口的路由，这里使用了路由汇聚，2001:0:0:8::/62 是 2001:0:0:8::/64、
2001:0:0:9::/64、2001:0:0:10::/64、2001:0:0:11::/64 四条路由的精确汇总，IPv6 路由的汇总
方法和 IPv4 相同。
R2(config)#ipv6 route 2001:0:0:4::/64 2001:0:0:3::2 去往 R3 环回接口的路由。
```

R3 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#ipv6 unicast-routing
R3(config)#int s1/0
R3(config-if)#ipv6 address 2001:0:0:3::2/64
R3(config-if)#no shut
R3(config)#int lo0
R3(config-if)#ipv6 address 2001:0:0:4::1/64
R3(config-if)#exit
R3(config)#ipv6 route ::0 2001:0:0:3::1
```

配置完成后，在 R1、R2、R3 上任意 ping 图中标出的所有 IPv6 地址，应该都可以 ping 通。

2. 动态路由的配置

RIP、OSPF 等路由协议都有针对 IPv6 的版本，CCNA 考试中只需要了解 RIPng (Routing Information Protocol next generation，RIP 下一代版本) 动态路由即可。

RIPng 和 RIPv2 非常相似，也是一个距离矢量的路由协议，最大跳数是 15，使用水平分割和毒性反转来阻止路由环路。RIPng 使用多播地址 FF02::9 作为目的更新地址，发送更新使用的是 UDP 协议的 521 端口。下面使用 RIPng 来配置图 21-3-1。

实验 21-2：配置 IPv6 RIPng

R1 的配置如下（斜体部分是注释）：

```
Router>en
```

```

Router#conf t
Router(config)#host R1
R1(config)#ipv unicast-routing
R1(config)#int s1/1
R1(config-if)#ipv add 201:0:0:2::1/64
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ipv add 2001:0:0:8::1/64
RR1(config-if)#ipv add 2001:0:0:9::1/64
R1(config-if)#ipv add 2001:0:0:10::1/64
R1(config-if)#ipv add 2001:0:0:11::1/64
R1(config-if)#exit
R1(config)#ipv6 router rip test  启用RIPng 协议，这里的test 是随便起的一个名字，就像OSPF
                                的进程号一样，只具有本地意义。

R1(config-rtr)#int lo0
R1(config-if)#ipv6 rip test enable
RIPng 不同于RIP，不是在路由进程下宣告所有的直连网络，而是在接口宣告这个接口运行RIPng 协议，这里
的test 要与路由进程中的名字一致。
R1(config-if)#int s1/1
R1(config-if)#ipv6 rip test enable

```

R2 的配置如下（斜体部分是注释）：

```

Router>en
Router#conf t
Router(config)#host R2
R2(config)#ipv unicast-routing
R2(config)#int s1/0
R2(config-if)#ipv ad 2001:0:0:2::2/64
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ipv add 2001:0:0:3::1/64
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ipv6 router rip abc  这里的abc 同样只具有本地意义，不同的路由器上的名字不要求一
                                样，可以随便输入。

R2(config-rtr)#int s1/1
R2(config-if)#ipv rip abc enable
R2(config-if)#int s1/0
R2(config-if)#ipv rip abc enable

```

R3 的配置如下：

```

Router>en
Router#conf t
Router(config)#host R3
R3(config)#ipv unicast-routing
R3(config)#int s1/0
R3(config-if)#ipv ad 2001:0:0:3::2/64
R3(config-if)#no shut
R3(config-if)#int lo0
R3(config-if)#ipv add 2001:0:0:4::1/64
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ipv router rip test
R3(config-rtr)#int s1/0
R3(config-if)#ipv rip test enable
R3(config-if)#int lo0
R3(config-if)#ipv rip test enable

```

配置完成后，在 R1、R2、R3 上任意 ping 图中标出的所有 IPv6 地址，应该都可以 ping 通。在 R3 上执行“show ipv6 route”命令，显示如下：

```

R3#show ipv6 route
IPv6 Routing Table - 11 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route

```

```

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R 2001:0:0:2::/64 [120/2]
  via FE80::C808:FF:FE98:0, Serial1/0
C 2001:0:0:3::/64 [0/0]
  via ::, Serial1/0
L 2001:0:0:3::2/128 [0/0]
  via ::, Serial1/0
C 2001:0:0:4::/64 [0/0]
  via ::, Loopback0
L 2001:0:0:4::1/128 [0/0]
  via ::, Loopback0
R 2001:0:0:8::/64 [120/3]
  via FE80::C808:FF:FE98:0, Serial1/0
R 2001:0:0:9::/64 [120/3]
  via FE80::C808:FF:FE98:0, Serial1/0
R 2001:0:0:10::/64 [120/3]
  via FE80::C808:FF:FE98:0, Serial1/0
R 2001:0:0:11::/64 [120/3]
  via FE80::C808:FF:FE98:0, Serial1/0
L FE80::/10 [0/0]
  via ::, Null0
L FF00::/8 [0/0]
  via ::, Null0

```

从这里的输出中可以看到，RIPng 的跳数比想象的多 1 跳，这是 RIPng 与 RIP 不同的地方，在 RIPng 中，在默认情况下，进入路由选择表之前 RIPng 度量值加 1；还可以看到 RIPng 的下一跳不是邻居接口的 IP 地址，而是一个 FE80::/64 的地址，这个地址就是邻居路由器的链路本地地址，RIPng 使用链路本地地址作为更新消息的源地址，在 IPv6 路由表中的下一跳是使用链路本地地址表示的；也可以看到路由表中还多出一些 L 开头的路由，不用理会，更多的讨论已超出 CCNA 的考试范围。



21.4 IPv6 过渡策略***

所有结点不可能在同一时间从 IPv4 过渡到 IPv6，这需要一个过渡期，在这个过渡期内，IPv4 与 IPv6 共存。有许多过渡机制，以便顺利整合 IPv4 与 IPv6。也有些机制，可以允许 IPv4 的结点与 IPv6 结点互相通信。在不同的情况下需要不同的策略，下面是一些可供选择的过渡策略。

1. 双栈（Dual Stacking）

双栈是一种集成方法，也就是双协议。一个结点可以和 IPv4 的结点连接和通信，也可以和 IPv6 的结点连接和通信。在同一时间内既要运行 IPv4，又要运行 IPv6 的情况下，这种方法被推荐使用。

在图 21-4-1 中，路由器的 fa0/0 接口既有 IPv4 的网络，又有 IPv6 的网络，该路由器既支持 IPv4，又支持 IPv6。

2. 隧道（Tunneling）

有几种隧道技术可以使用，包括：

- 手动 IPv6-over-IPv4 隧道：一个 IPv6 的包被封装在 IPv4 协议内。这种方法需要双栈路由器。
- 动态 6to4 隧道：通过 IPv4 的网络自动连接 IPv6 的孤岛，通常是在互联网上。这种

方法为每一个 IPv6 的孤岛动态应用一个合法的、唯一的 IPv6 前缀，可以在企业网络中快速地部署 IPv6，而不需要从 ISP 运营商或注册机构获取 IP 地址。

除上面两种隧道技术外，还有一些比较冷门的隧道技术，包括：

- 内部网站自动隧道处理协议隧道（Intra-Site Automatic Tunnel Addressing Protocol, ISATAP）：自动覆盖隧道机制，利用下部的 IPv4 网络作为 IPv6 的一个链路层。
- Teredo 隧道（Teredo tunneling）：一个 IPv6 过渡技术，提供主机到主机的自动隧道而不是网关的隧道。

3. NAT 的协议转换（NAT-PT）

直接转换使用不同版本 IP 协议的主机，使它们之间可以通信。这种转换比 IPv4 的转换技术要复杂。现在，这种翻译技术是最不受欢迎的选择，被用做最后的选择。

有一个建议是：可以使用双栈的地方一定可以使用隧道，双栈和隧道是两种最常见的 IPv4 向 IPv6 的过渡技术。

实验 21-3：配置 IPv6-over-IPv4 隧道

在图 21-4-2 中，R1 左边和 R3 右边是 IPv6 的网络，中间是 IPv4 的网络，R2 只支持 IPv4 路由或没有运行 IPv6 路由。当前很多网络都存在这种情况，两端运行的是 IPv6 网络，中间是 IPv4 网络。那么如何实现两端 IPv6 网络的通信呢？这里介绍一种 IPv6-over-IPv4 隧道技术的配置。

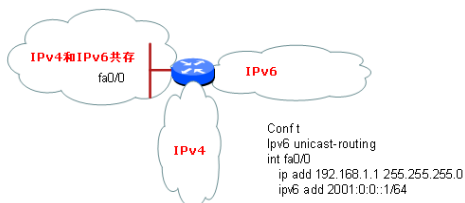


图 21-4-1 双栈

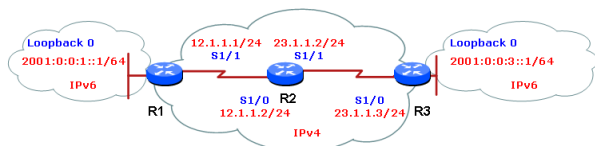


图 21-4-2 IPv6-over-IPv4 隧道

R1 的配置如下（斜体部分是注释）：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#ipv6 unicast-routing
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ipv6 address 2001:0:0:1::1/64
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.2
R1(config)#int tunnel 0
R1(config-if)#tunnel source s1/1
R1(config-if)#tunnel destination 23.1.1.3
R1(config-if)#tunnel mode ipv6ip
R1(config-if)#ipv6 address 2001:0:0:2::1/64
R1(config-if)#exit
```

创建一个隧道端口。

隧道的地址是本路由器的 S1/1，或者写成 IP 地址 12.1.1.1 也可以。

隧道的目的地址，这里只能写成隧道终点路由器接口的 IP 地址，这里是 R3 的 S1/0 的 IP 地址，即 23.1.1.3。为了使隧道能正常工作，R1 一定能到达 23.1.1.3，也就是说，IPv4 的路由要可达，不然隧道建立不起来。

隧道的模式是 IPv6-over-IPv4，也就是把 IPv6 的包封装在 IPv4 的包中。

给隧道端口配置一个 IPv6 的地址。

```
R1(config)#ipv6 route ::/0 2001:0:0:2::2
```

配置 IPv6 的路由。

R2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
```

R3 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#ipv6 unicast-routing
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo0
R3(config-if)#ipv6 add 2001:0:0:3::1/64
R3(config-if)#int tun 0
R3(config-if)#tunnel source s1/0 在 R3 上隧道的源和目的地址刚好与 R1 上的相反。
R3(config-if)#tunnel destination 12.1.1.1
R3(config-if)#tunnel mode ipv6ip
R3(config-if)#ip add 2001:0:0:2::2/64
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 23.1.1.2
R3(config)#ipv6 route ::/0 2001:0:0:2::1
R3(config)#exit
```

配置完成后, 在 R3 上 ping 路由器 R1 上的 IPv6 地址, 结果如下, 可以发现能够 ping 通。

```
R3#ping 2001:0:0:1::1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:0:0:1::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 288/464/700 ms
R3#
```

经过上述配置后, 两个 IPv6 的网络可以穿越 IPv4 进行传输。图中的 R2, 也就是 IPv4 网络对此并不知情, 可以说是透明传输。



21.5 真题精选*

1. Which two statements are true concerning IPv6? (Choose two.)

- A. Mobile IP is built into IPv6 by default.
- B. The leading zeros in an address format are mandatory.
- C. Like IPv4, IPv6 broadcasts are sent to all nodes on a LAN segment.
- D. IPSec is mandatory and built into IPv6.

2. Which statement about IPv6 is true?

- A. Addresses are not hierarchical and are assigned at random.
- B. Only one IPv6 address can exist on a given interface.
- C. There are 2.7 billion addresses available.
- D. Broadcasts have been eliminated and replaced with multicasts.

3. Which three IPv6 notations represent the same address? (Choose three.)
 - A. 2031:0000:130F:0000:0000:09C0:876A:130B
 - B. 2031::130F::9C0:876A:130B
 - C. 2031:0:130F::9C0:876A:130B
 - D. 2031::130F:0::9C0:876A:130B
 - E. 2031:0:130F:0:0:09C0:876A:130B
 - F. 2031:0:130F::9C0:876A:130B
4. What number is a valid representation for the 200F:0000:0000:AB00:0000:0000:0000:0000/56 IPv6 prefix?
 - A. 200F:0:0:AB/56
 - B. 200F:0:0:AB00::/56
 - C. 200F::AB00/56
 - D. 200F::AB/56
5. Which option is a valid IPv6 address?
 - A. 2001:0000:130F::099a::12a
 - B. 2002:7654:A1AD:61:81AF:CCCC
 - C. FEC0:ABCD:WXYZ:0067::2A4
 - D. 2004:1:25A4:886F::1
6. Which address type does the IPv6 address FF05:0:0:0:0:0:2 specify?
 - A. unspecified
 - B. aggregable global unicast
 - C. link local
 - D. site local unicast
 - E. multicast
7. How many bits are contained in each field of an IPv6 address?
 - A. 24
 - B. 4
 - C. 8
 - D. 16
8. Which two statements describe characteristics of IPv6 unicast addressing? (Choose two.)
 - A. Global addresses start with 2000::/3.
 - B. Link-local addresses start with FE00::/12.
 - C. Link-local addresses start with FF00::/10.
 - D. There is only one loopback address and it is ::1.
 - E. If a global address is assigned to an interface, then that is the only allowable address for the interface.
9. What is known as "one-to-nearest" addressing in IPv6?
 - A. global unicast
 - B. anycast
 - C. multicast
 - D. unspecified address
10. Which two of these statements are true of IPv6 address representation? (Choose two.)
 - A. There are four types of IPv6 addresses: unicast, multicast, anycast, and broadcast.
 - B. A single interface may be assigned multiple IPv6 addresses of any type.
 - C. Every IPv6 interface contains at least one loopback address.
 - D. The first 64 bits represent the dynamically created interface ID.
 - E. Leading zeros in an IPv6 16 bit hexadecimal field are mandatory.

11. Running both IPv4 and IPv6 on a router simultaneously is known as what?

- A. 4to6 routing
- B. 6to4 routing
- C. binary routing
- D. dual-stack routing
- E. NextGen routing

12. Which three techniques can be used to transition from IPv4 to IPv6? (Choose three.)

- A. 6to4 tunneling
- B. flow label
- C. dual stack
- D. anycast
- E. NAT
- F. mobile IP

13. Which term describes the process of encapsulating IPv6 packets inside IPv4 packets?

- A. tunneling
- B. hashing
- C. routing
- D. NAT

14. What are three IPv6 transition mechanisms? (Choose three.)

- A. 6to4 tunneling
- B. VPN tunneling
- C. GRE tunneling
- D. ISATAP tunneling
- E. PPP tunneling
- F. Teredo tunneling



21.6 真题解答*

1. 解: AD

题目问: 关于 IPv6, 哪两个语句是正确的? 参照本章 21.1 节的描述, IPv6 默认支持移动和安全。故 A 和 D 正确。

2. 解: D

题目问: 关于 IPv6, 哪个语句是正确的? A 选项说 IPv6 地址没有层次性, 并且可以随机分配, 显然是错误的, IPv6 有层次性且被严格分配。B 选项说只有一个 IPv6 地址可以存在一个接口上, 事实上, 不同类型的多个 IPv6 地址可以被同时配置在一个接口上。C 选项说有 27 亿个 IPv6 地址, 事实上约有 3.4×10^{38} 个, 远不止这么多。D 选项说 IPv6 中取消的广播, 被组播代替。

3. 解: ACE

题目问: 哪三个 IPv6 符号表示的是同一个地址(选 3 个)? A 是一个完整的 IPv6 地址, 包含 128 个比特, 每 16 个比特用一个十六进制数表示, 共有 8 个部分。IPv6 每一部分的前导 0 可以省略, 则 E 和 A 是同一个地址。IPv6 连续的多个全 0 部分可以用::表示, 为了避免指代不清, 这种表示法只能使用一次, C 和 A 也是一个地址。故 A、C 和 E 正确。

4. 解: B

题目问: 200F:0000:0000:AB00:0000:0000:0000/56 可以怎么表示 IPv6 前缀? 问的是如何表示 IPv6 的网络地址, A 选项相当于 200F:0:0:00AB/56, C 选项是 200F::/56, D 选项也是 200F::/56。正确的答案只有 B。

5. 解: D

题目问: 哪一个是合法的 IPv6 地址? A 选项“::”简写出现了两次, 在同一个 IPv6 地址中, 这种简写只能出现一次。B 选项中的位数只有 96 位, 不足 128 位。C 选项中出现了 WXYZ 字符, 十六制中最大只会出现字母 F。故只有 D 正确。

6. 解：E

题目问：FF05:0:0:0:0:0:2 是 IPv6 中的哪一种地址类型？FF/8 是 IPv6 中的组播地址，有时也称多播。更细地说，FF05 打头的是永久性的站点组播地址。

7. 解：D

题目问：IPv6 的每一个域中包含多少个比特。IPv6 采用冒号分十六进制数表示，分成 8 个部分，每个部分有 16 个比特。

8. 解：AD

题目问：哪两个语句描述了 IPv6 单播地址的特点？链路本地地址以 FE80/10 开始，故选项 B 和 C 都错。E 选项说一个接口只能有一个 IPv6 地址，也是错误的。

9. 解：B

题目问：在 IPv6 中什么被认为是"one-to-nearest"地址？这里指的是任意播地址。

10. 解：BC

题目问：在 IPv6 的地址表示中，哪两个语句是正确的？A 选项说 IPv6 中有广播，显然错误。B 选项说一个接口可以被配置任意类型的多个 IPv6 地址，是正确的。C 选项说每个接口至少包含一个环回地址，从书中的“实验 21-2：配置 IPv6 RIPng”输出的 IPv6 路由表可以得出这一结论。D 选项中，应该是后 64 比特，不是前 64 比特。E 选项说 IPv6 中每 16 个比特的十六进制数表示法中，前导 0 不能省略，其实是可以省略的。

11. 解：D

题目问：一台路由器同时运行 IPv4 和 IPv6 被叫做什么？答案是 D，双栈。

12. 解：ACE

题目问：从 IPv4 向 IPv6 转换，哪三种技术可以被使用？参照本章 2.4 节，A、C 和 E 正确。

13. 解：A

题目问：哪个术语描述了封装 IPv6 数据包到 IPv4 数据包的方法？答案是隧道。

14. 解：ADF

题目问：什么是 IPv6 的三种转换机制？对照本章的 21.4 节，可知正确答案是 ADF。

第 22 章

综合实验***

本章通过完成一个综合实验，来检验读者对路由器和交换机的基本配置、设备的远程管理、VLAN 的划分、VTP 协议的使用、STP 协议的配置、动态/静态路由协议的配置、DHCP 的配置、NAT 的配置、PPP 的配置及 ACL 应用的掌握情况。

22.1 实验要求**

某企业通过路由器 R1 接入 Internet，R2、R3 和 R4 模拟 Internet 中的网云，整个网络的拓扑如图 22-1-1 所示。

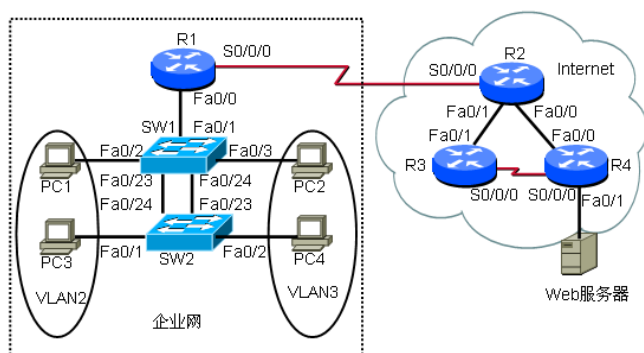


图 22-1-1 综合实验拓扑

各设备的 IP 地址配置如下。

R1:

S0/0/0: 12.1.1.1/24
Fa0/0.1: 192.168.1.1/24
Fa0/0.2: 192.168.2.1/24
Fa0/0.3: 192.168.3.1/24

R2:

S0/0/0: 12.1.1.2/24
Fa0/0: 24.1.1.2/24
Fa0/1: 23.1.1.2/24

R3:

S0/0/0: 34.1.1.3/24

Fa0/1: 23.1.1.3/24

R4:

S0/0/0: 34.1.1.4/24

Fa0/0: 24.1.1.4/24

Fa0/1: 218.1.1.1/24

SW1:

VLAN 1: 192.168.1.2/24

SW2:

VLAN 1: 192.168.1.3/24

PC1、PC2、PC3 和 PC4 的 IP 地址均自动获取。PC1 和 PC3 属于 VLAN2，VLAN2 所在的 IP 子网是 192.168.2.0/24。PC2 和 PC4 属于 VLAN3，VLAN3 所在的 IP 子网是 192.168.3.0/24。

Web 服务器: 218.1.1.2/24

要求:

(1) 在 Packet Tracer 模拟器中绘制如图 22-1-1 所示的拓扑，注意设备之间线缆类型的选择；或者打开光盘中的“配置\22\综合实验.pkt”文件。完成后的拓扑如图 22-1-2 所示。

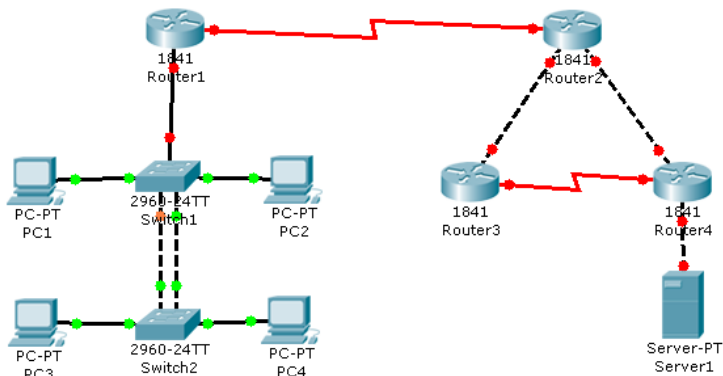


图 22-1-2 Packet Tracer 模拟拓扑

(2) 根据拓扑要求为每个设备配置 IP 地址，保证所有配置的接口状态为 UP。

(3) 配置设备的远程登录和密码保护。配置图中的 2 台交换机、4 台路由器，使 6 台设备均支持远程登录和配置，配置中出现的所有密码均使用 cisco，并且不能在配置文件中明文显示。

(4) 配置 VTP 协议。配置 SW1 为 VTP Server，SW2 为 VTP Client。

(5) VLAN 配置。在 SW1 上配置 VLAN，保证 SW2 可以使用 VTP 协议从 SW1 上同步 VLAN 配置信息。配置 4 台 PC 到对应的 VLAN。配置路由器 R1 的子接口，使其支持 VLAN 间路由。

(6) 配置 STP 协议。配置生成树协议，使 SW1 为根交换机。

(7) 配置 DHCP。在路由器 R1 上配置 DHCP，使 4 台 PC 都可以获取到正确的 IP 地址、网关和 DNS，DNS 服务器的地址是 218.1.1.2。

(8) 配置路由协议。配置 R1，使其可以访问 Internet。配置 R2、R3 和 R4 运行 OSPF

路由协议。配置完成后，4 台路由器之间相互都可访问。

(9) 配置 PPP 协议。路由器 R1 与 R2 之间封装的协议是 PPP，使用 CHAP 验证，密码仍然是 cisco。

(10) 配置 NAT。在路由器 R1 上配置动态 PAT，使 4 台 PC 都可以通过 R1 访问 Internet。在路由器 R1 上配置静态 PAT，使 Internet 可以通过路由器 R1 的 TCP 2323 端口 Telnet 登录到 SW1。

(11) 配置 ACL。配置路由器 R1，拒绝 VLAN2 的主机访问 Web 服务器的 WWW 服务，其他服务不受影响。



22.2 实验配置***

根据上一节的实验要求，本节来完成实验配置。

(1) 在 Packet Tracer 模拟器中打开光盘中的“配置\22\综合实验.pkt”文件。图中使用了 5 根交叉双绞线、5 根直通双绞线、2 根串行线，R1 和 R3 是串行线缆的 DCE 端。

(2) 配置 IP 地址。

● 配置

R1 的配置如下，这里仅配置 S0/0/0 接口的 IP 地址，并打开 Fa0/0 接口，每个子接口 IP 地址的配置属于 VLAN 配置部分。

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s0/0/0
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shut
R1(config-if)#int fa 0/0
R1(config-if)#no shut
```

R2 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s0/0/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int fa 0/0
R2(config-if)#ip add 24.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int fa 0/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
```

R3 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s0/0/0
R3(config-if)#ip add 34.1.1.3 255.255.255.0
R3(config-if)#clock rate 64000
R3(config-if)#no shut
R3(config-if)#int fa 0/1
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
```

R4 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R4
R4(config)#int s0/0/0
R4(config-if)#ip add 34.1.1.4 255.255.255.0
R4(config-if)#no shut
R4(config-if)#int fa 0/0
R4(config-if)#ip add 24.1.1.4 255.255.255.0
R4(config-if)#no shut
R4(config-if)#int fa 0/1
R4(config-if)#ip add 218.1.1.1 255.255.255.0
R4(config-if)#no shut
```

SW1 的配置如下:

```
Switch>en
Switch#conf t
Switch(config)#host SW1
SW1(config)#int vlan 1
SW1(config-if)#ip add 192.168.1.2 255.255.255.0
SW1(config-if)#no shut
SW1(config-if)#exit
SW1(config)#ip default-gateway 192.168.1.1
```

SW2 的配置如下:

```
Switch>en
Switch#conf t
Switch(config)#host SW2
SW2(config)#int vlan 1
SW2(config-if)#ip add 192.168.1.3 255.255.255.0
SW2(config-if)#no shut
SW2(config-if)#exit
SW2(config)#ip default-gateway 192.168.1.1
```

PC1、PC2、PC3 和 PC4 的地址是自动获取, 等配置完 DHCP 后再来查看。

Web 服务器的配置如下:

IP 地址: 218.1.1.2

掩码: 255.255.255.0

网关: 218.1.1.1

• 检验

IP 地址配置完成后, 可以使用“show ip interface brief”命令进行检查, 看所有接口 IP 地址的配置和接口的状态。比如路由器 R2 的执行和显示如下:

```
R2#show ip int brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 24.1.1.2        YES manual up          up
FastEthernet0/1 23.1.1.2        YES manual up          up
Serial0/0/0     12.1.1.2        YES manual up          up
Serial0/0/1     unassigned      YES manual administratively down down
Vlan1           unassigned      YES manual administratively down down
```

在所有的设备上 ping 所有直连设备与本设备直连接口的 IP 地址, 测试网络的连通性。比如在 R2 上 ping 其中一个直连设备 R1, 测试直连网络的连通性, 显示如下:

```
R2#ping 12.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/38/47 ms
```

(3) 配置设备的远程登录和密码保护。

- 配置

R1 的配置如下：

```
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable secret cisco
R1(config)#service password-encryption
```

R2、R3、R4、SW1 和 SW2 的配置与 R1 的配置类似，读者可以在记事本中输入下面的内容，然后在每个设备上粘贴，来节省配置时间。

```
en
conf t
line vty 0 4
password cisco
login
enable secret cisco
service password-encryption
```

- 检验

在路由器 R2 上远程登录路由器 R1，操作和显示如下：

```
R2#telnet 12.1.1.1
Trying 12.1.1.1 ...

User Access Verification

Password:
R1>en
Password:
R1#
```

在路由器 R2 上使用“show running-config”命令查看密码的显示情况，关键部分的显示如下：

```
R2#show run
省略部分输出。
line vty 0 4
 password 7 0822455D0A16
 login
end
R2#
```

(4) 配置 VTP 协议。

- 配置

SW1 的配置如下：

```
SW1(config)#vtp domain ccna
SW1(config)#int fa 0/23
SW1(config-if)#switchport mode trunk
SW1(config-if)#int fa 0/24
SW1(config-if)#swi mode trunk
```

SW2 的配置如下：

```
SW2(config)#vtp domain ccna
SW2(config)#vtp mode client
SW2(config)#int fa 0/23
SW2(config-if)#swi mode trunk
SW2(config-if)#int fa 0/24
SW2(config-if)#swi mode trunk
```


因为思科交换机默认是 VTP Server，所以 SW1 只要配置 VTP 域名就可以了。特别要注意的是，VTP 信息只能在 Trunk 链路上传输，SW1 和 SW2 之间的两条链路要配置成主干链路。

• 检验

配置完成后，在 SW2 上使用“show vtp status”命令进行查看，显示结果如下：

```
SW2#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 64
Number of existing VLANs    : 5
VTP Operating Mode          : Client
VTP Domain Name             : ccna
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xE1 0x2A 0x13 0xE5 0xB3 0xA4 0x96 0xA4
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

因为 SW1 上还没有配置 VLAN 信息，SW1 上 VTP 的配置修正号是 0，所以 SW2 的配置修正号也是 0，存在的 VLAN 个数仍然是默认的 5 个。配置完 VLAN 后，可以进一步检验 VTP 的配置。

(5) VLAN 配置。

• 配置 VLAN

在 VTP Server 交换机 SW1 上添加 VLAN，并把端口加入对应的 VLAN 中。SW1 的配置如下：

```
SW1(config)#vlan 2
SW1(config-vlan)#vlan 3
SW1(config-vlan)#int fa 0/2
SW1(config-if)#swi mode acc
SW1(config-if)#swi acc vlan 2
SW1(config-if)#int fa 0/3
SW1(config-if)#swi mode acc
SW1(config-if)#swi acc vlan 3
```

配置完成后，使用“show vlan”命令检查 SW1 上 VLAN 的配置情况，显示如下：

```
SW1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Gig1/1, Gig1/2
2	VLAN0002	active	Fa0/2
3	VLAN0003	active	Fa0/3
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

使用“show vtp status”命令检查 SW1 上的 VTP 信息，显示如下：

```
SW1#show vtp status
VTP Version                : 2
Configuration Revision      : 2
Maximum VLANs supported locally : 64
Number of existing VLANs    : 7
VTP Operating Mode          : Server
VTP Domain Name             : ccna
```

```
VTP Pruning Mode           : Disabled
VTP V2 Mode               : Disabled
VTP Traps Generation      : Disabled
MD5 digest                : 0x0A 0xCA 0xA5 0x9F 0x1C 0x97 0x85 0x1A
Configuration last modified by 192.168.1.2 at 3-1-93 01:11:08
Local updater ID is 192.168.1.2 on interface Vl1 (lowest numbered VLAN interface found)
```

注意到 VTP 的配置修正号变成了 2, 存在的 VLAN 数也变成了 7。使用“show vtp status”命令检查 SW2 上的 VTP 信息, 显示如下:

```
SW2#show vtp status
VTP Version                : 2
Configuration Revision      : 2
Maximum VLANs supported locally : 64
Number of existing VLANs    : 7
VTP Operating Mode         : Client
VTP Domain Name            : ccna
VTP Pruning Mode           : Disabled
VTP V2 Mode               : Disabled
VTP Traps Generation      : Disabled
MD5 digest                : 0x0A 0xCA 0xA5 0x9F 0x1C 0x97 0x85 0x1A
Configuration last modified by 192.168.1.2 at 3-1-93 01:11:08
```

从上面的输出中可以看到, SW2 上的 VLAN 配置信息与 SW1 的 VLAN 配置信息同步。VTP 仅能同步 VLAN 信息, VLAN 中包含的端口还需要单独配置。SW2 的配置如下:

```
SW2(config)#int fa 0/1
SW2(config-if)#swi mode acc
SW2(config-if)#swi acc vlan 2
SW2(config-if)#int fa 0/2
SW2(config-if)#swi mode acc
SW2(config-if)#swi acc vlan 3
```

• 配置 VLAN 间路由

这里要配置单臂路由, 借助路由器 R1 实现 VLAN1、VLAN2、VLAN3 之间的互访。SW1 和 R1 之间的链路要配置成主干链路, SW1 的配置如下:

```
SW1(config)#int fa 0/1
SW1(config-if)#swi mode trunk
```

路由器 R1 的配置如下:

```
R1(config)#int fa 0/0.1
R1(config-subif)#encapsulation dot1Q 1
R1(config-subif)#ip add 192.168.1.1 255.255.255.0
R1(config-subif)#int fa 0/0.2
R1(config-subif)#enca dot 2
R1(config-subif)#ip add 192.168.2.1 255.255.255.0
R1(config-subif)#int fa 0/0.3
R1(config-subif)#enca dot 3
R1(config-subif)#ip add 192.168.3.1 255.255.255.0
```

• 检验

因为 4 台 PC 还没有配置 IP 地址, 等配置完 DHCP 后, 再测试 VLAN 间路由是否成功。(6) 配置 STP 协议。要求配置生成树协议, 使 SW1 为根交换机。

• 配置

配置前先查看 STP 协议的运行情况。SW1 上的显示如下:

```
SW1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address     0001.6359.386A
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```

Bridge ID Priority    32769 (priority 32768 sys-id-ext 1)
Address          0006.2A10.DE01
Aging Time 300

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Desg FWD 19      128.3   Shr
Fa0/23         Altn BLK 19      128.3   Shr
Fa0/24         Root FWD 19      128.3   Shr

VLAN0002
Spanning tree enabled protocol ieee
Root ID      Priority    32770
Address      0001.6359.386A
Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID    Priority    32770 (priority 32768 sys-id-ext 2)
Address      0006.2A10.DE01
Aging Time 300

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Desg FWD 19      128.3   Shr
Fa0/2          Desg FWD 19      128.3   Shr
Fa0/23         Altn BLK 19      128.3   Shr
Fa0/24         Root FWD 19      128.3   Shr

VLAN0003
Spanning tree enabled protocol ieee
Root ID      Priority    32771
Address      0001.6359.386A
Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID    Priority    32771 (priority 32768 sys-id-ext 3)
Address      0006.2A10.DE01
Aging Time 300

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Desg FWD 19      128.3   Shr
Fa0/3          Desg FWD 19      128.3   Shr
Fa0/23         Altn BLK 19      128.3   Shr
Fa0/24         Root FWD 19      128.3   Shr

SW1#

```

从上面的输出中可以看到，交换机上默认运行的是 PVST+（Per Vlan Spanning Tree +，Catalyst 交换机上 STP 默认模式是 PVST+，PVST+ 模式为每一个 VLAN 运行一个 STP 实例），在 VLAN1、VLAN2 和 VLAN3 中，SW1 都不是根交换机，交换机上使用了扩展的 system-ID，system-ID 等于每个 VLAN 的编号。SW1 的 Fa0/24 是根端口，Fa0/23 端口被阻塞。

网络中只有两台交换机，既然 SW1 不是根交换机，那么根交换机是 SW2。配置 SW1，使其成为所有 VLAN 的根交换机，配置命令如下：

```
SW1(config)#spanning-tree vlan 1,2,3 priority 4096
```

• 检验

配置完成后，在 SW1 上再次查看生成树协议的运行情况，显示如下：

```

SW1#show spanning-tree

VLAN0001
Spanning tree enabled protocol ieee
Root ID      Priority    4097
Address      0006.2A10.DE01

```

```

This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 4097 (priority 4096 sys-id-ext 1)
Address 0006.2A10.DE01
Aging Time 300

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.3	Shr
Fa0/23	Desg	LSN	19	128.3	Shr
Fa0/24	Desg	FWD	19	128.3	Shr

省略部分输出。

注意，此时 SW1 已经是根交换机了。

(7) 配置 DHCP。

• 配置

路由器 R1 的配置如下：

```

R1(config)#ip dhcp excluded-address 192.168.2.1
R1(config)#ip dhcp pool vlan2
R1(dhcp-config)#network 192.168.2.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.2.1
R1(dhcp-config)#dns-server 218.1.1.2
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 192.168.3.1
R1(config)#ip dhcp pool vlan3
R1(dhcp-config)#network 192.168.3.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.3.1
R1(dhcp-config)#dns-server 218.1.1.2

```

• 检验

使用如图 22-2-1 所示的方法，依次配置 PC1、PC2、PC3 和 PC4，使用 DHCP 分配。



图 22-2-1 配置 PC 自动获取 IP 地址

配置完成后，在 PC1 的 DOS 窗口中查看 IP 地址的获取情况，显示如下：

```

PC>ipconfig /all

Physical Address.....: 0090.2B67.6125
IP Address.....: 192.168.2.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.1
DNS Servers.....: 218.1.1.2

```

使用类似的方法，可以查看到 PC2 的 IP 地址是：192.168.3.2，PC3 的 IP 地址是：192.168.2.3，PC4 的 IP 地址是：192.168.3.3，这表明 DHCP 配置正确。在 PC1 上 ping PC2 的 IP 地址，显示如下：

```
PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=160ms TTL=127
Reply from 192.168.3.2: bytes=32 time=170ms TTL=127
Reply from 192.168.3.2: bytes=32 time=169ms TTL=127
Reply from 192.168.3.2: bytes=32 time=162ms TTL=127

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 160ms, Maximum = 170ms, Average = 165ms
```

PC1 能成功地 ping 通 PC2，表明前面配置的 VLAN 间路由正确。在 PC1 上 ping PC3，显示如下：

```
PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=227ms TTL=128
Reply from 192.168.2.3: bytes=32 time=114ms TTL=128
Reply from 192.168.2.3: bytes=32 time=150ms TTL=128
Reply from 192.168.2.3: bytes=32 time=117ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 114ms, Maximum = 227ms, Average = 152ms
```

PC1 能成功地 ping 通 PC3，表明前面配置的跨交换机 VLAN 内的通信也正确。

(8) 配置路由协议。

● 配置

在路由器 R1 上配置默认路由，把所有未知流量都发往 Internet，配置命令如下：

```
R1(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.2
```

配置 R2、R3 和 R4，运行 OSPF 路由协议。R2 的配置如下：

```
R2(config)#router ospf 1
R2(config-router)#net 24.1.1.0 0.0.0.255 area 0
R2(config-router)#net 23.1.1.0 0.0.0.255 area 0
R2(config-router)#net 12.1.1.0 0.0.0.255 area 0
```

R3 的配置如下：

```
R3(config)#router ospf 1
R3(config-router)#net 23.1.1.0 0.0.0.255 area 0
R3(config-router)#net 34.1.1.0 0.0.0.255 area 0
```

R4 的配置如下：

```
R4(config)#router ospf 1
R4(config-router)#net 24.1.1.0 0.0.0.255 area 0
R4(config-router)#net 34.1.1.0 0.0.0.255 area 0
R4(config-router)#net 218.1.1.0 0.0.0.255 area 0
```

● 检验

配置完成后，在路由器 R1 上依次 ping 图中模拟 Internet 部分的所有 IP 地址，应该都

可以 ping 通。在路由器 R1 上 ping Web 服务器，显示如下：

```
R1#ping 218.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 218.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 97/110/138 ms
```

读者还可以进一步查看 R2、R3 和 R4 的 OSPF 邻居表、路由表，验证配置无误。路由器 R2 的 OSPF 邻居表显示如下：

Neighbor ID	Pri	State	Dead Time	Address	Interface
218.1.1.1	1	FULL/BDR	00:00:37	24.1.1.4	FastEthernet0/0
34.1.1.3	1	FULL/DR	00:00:38	23.1.1.3	FastEthernet0/1

路由器 R2 的路由表显示如下：

```
R2#show ip route
 12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial0/0/0
 23.0.0.0/24 is subnetted, 1 subnets
C    23.1.1.0 is directly connected, FastEthernet0/1
 24.0.0.0/24 is subnetted, 1 subnets
C    24.1.1.0 is directly connected, FastEthernet0/0
 34.0.0.0/24 is subnetted, 1 subnets
O    34.1.1.0 [110/65] via 24.1.1.4, 00:02:28, FastEthernet0/0
      [110/65] via 23.1.1.3, 00:02:18, FastEthernet0/1
O    218.1.1.0/24 [110/2] via 24.1.1.4, 00:02:28, FastEthernet0/0
```

(9) 配置 PPP 协议。

● 配置

路由器 R1 的配置如下：

```
R1(config)#user R2 pass cisco
R1(config)#int s0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
```

路由器 R2 的配置如下：

```
R2(config)#user R1 pass cisco
R2(config)#int s0/0/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
```

● 检验

关闭路由器 R1 的 S0/0/0 接口，稍后再次打开该接口，触发 PPP 的 CHAP 验证。

```
R1(config)#int s0/0/0
R1(config-if)#shut
R1(config-if)#no shut
R1(config-if)#^Z
R1#ping 12.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/34/52 ms
```

R1 可以成功 ping 通 R2，PPP 的 CHAP 验证成功。

(10) 配置 NAT。

● 配置

在路由器 R1 上配置动态 PAT，使 4 台 PC 都可以通过 R1 访问 Internet。R1 的配置如下：

```

R1(config)#int fa 0/0.2
R1(config-subif)#ip nat inside
R1(config-subif)#int fa 0/0.3
R1(config-subif)#ip nat inside
R1(config-subif)#int s0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#access-list 1 permit 192.168.2.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.3.0 0.0.0.255
R1(config)#ip nat inside source list 1 interface s0/0/0 overload

```

在路由器 R1 上配置静态 PAT，使 Internet 可以通过路由器 R1 的 TCP 2323 端口 Telnet 登录到 SW1。R1 的配置如下：

```

R1(config)#int fa 0/0.1
R1(config-subif)#ip nat inside
R1(config-subif)#exit
R1(config)#ip nat inside source static tcp 192.168.1.2 23 12.1.1.1 2323
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255

```

• 检验

在 PC1、PC2、PC3 和 PC4 上 ping Internet 中的地址。在 PC1 上 ping Web 服务器的 IP 地址，显示如下：

```

PC>ping 218.1.1.2

Pinging 218.1.1.2 with 32 bytes of data:

Reply from 218.1.1.2: bytes=32 time=207ms TTL=125
Reply from 218.1.1.2: bytes=32 time=192ms TTL=125
Reply from 218.1.1.2: bytes=32 time=228ms TTL=125
Reply from 218.1.1.2: bytes=32 time=203ms TTL=125

Ping statistics for 218.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 192ms, Maximum = 228ms, Average = 207ms

```

PC1 可以成功地 ping 通 Web 服务器。在路由器 R1 上使用“show ip nat translations”命令，查看路由器 R1 上配置的静态和产生的动态转换条目，显示如下：

```

R1#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 12.1.1.1:13        192.168.2.2:13    218.1.1.2:13      218.1.1.2:13
icmp 12.1.1.1:14        192.168.2.2:14    218.1.1.2:14      218.1.1.2:14
icmp 12.1.1.1:15        192.168.2.2:15    218.1.1.2:15      218.1.1.2:15
icmp 12.1.1.1:16        192.168.2.2:16    218.1.1.2:16      218.1.1.2:16
tcp 12.1.1.1:2323       192.168.1.2:23    ---               ---

```

从上面的输出中，可以看到 PC1 的私有 IP 地址 192.168.2.2，被转换成 12.1.1.1，然后可以成功到达公有网址 218.1.1.2，并能成功地返回。这表明动态 PAT 配置成功。

因为 Packet Tracer 模拟器中不支持带端口号的 telnet 命令，不然可以在路由器 R2、R3 或 R4 上执行“telnet 12.1.1.1 2323”命令，结果可以成功地远程登录到交换机 SW1 上。读者可以把 4 台 PC 中的一台换成服务器，然后在路由器 R1 上把 80 端口映射到该服务器，在路由器 R4 的 Fa0/1 接口接入交换机，然后添加一台 PC，并配置正确的 IP 地址，在 PC 的 IE 浏览器中输入 http://12.1.1.1 访问内网中的 Web 服务器。

(11) 配置 ACL。配置路由器 R1，拒绝 VLAN2 的主机访问 Web 服务器的 WWW 服务，其他服务不受影响。

- 配置

配置 ACL 前, 在 PC1 上访问 `http://218.1.1.2`, 显示如图 22-2-2 所示。

从图 22-2-2 中可以看到, PC1 可以成功地访问 Web 服务器的 WWW 服务。接下来配置 ACL, 路由器 R1 的配置如下:

```
R1(config)#access-list 100 deny tcp 192.168.2.0 0.0.0.255 host 218.1.1.2 eq 80
R1(config)#access-list 100 permit ip any any
R1(config)#int fa 0/0.2
R1(config-subif)#ip access-group 100 in
```

- 检验

配置完成后, 在 PC1 上访问 `http://218.1.1.2`, 显示如图 22-2-3 所示。

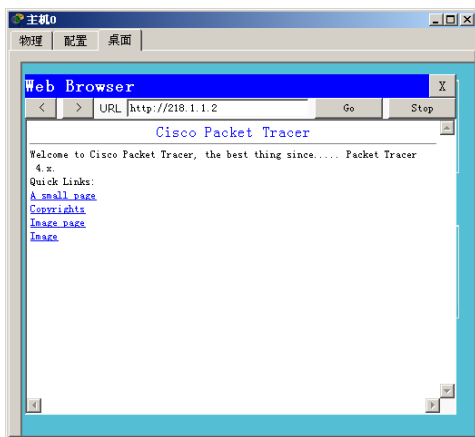


图 22-2-2 PC1 浏览 Web 服务器成功

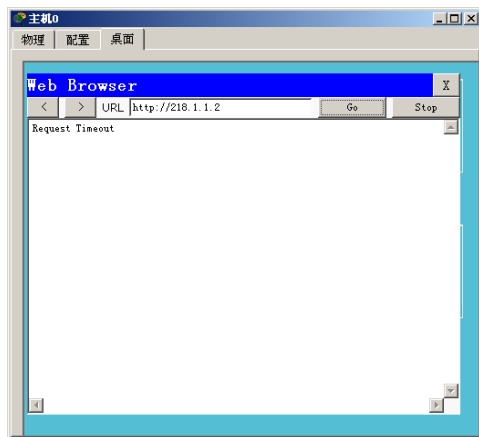


图 22-2-3 PC1 浏览 Web 服务器失败

PC1 访问 Web 服务器失败。在 PC1 上 ping Web 服务器的 IP 地址, 显示如下:

```
PC>ping 218.1.1.2

Pinging 218.1.1.2 with 32 bytes of data:

Reply from 218.1.1.2: bytes=32 time=214ms TTL=125
Reply from 218.1.1.2: bytes=32 time=178ms TTL=125
Reply from 218.1.1.2: bytes=32 time=224ms TTL=125
Reply from 218.1.1.2: bytes=32 time=195ms TTL=125

Ping statistics for 218.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 178ms, Maximum = 224ms, Average = 202ms
```

PC1 仍可以成功 ping 通 Web 服务器。

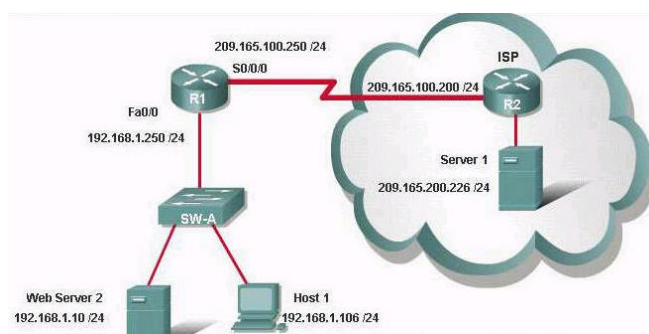
至此, 综合实验配置全部完成。



22.3 真题精选***

Refer to the topology:

The diagram represents a small network with a single connection to the Internet. Using the information shown, answer the following questions.



1. If the router R1 has a packet with a destination address 192.168.1.255, what describes the operation of the network?

- A. R1 will forward the packet out all interfaces.
- B. R1 will drop this packet because this it is not a valid IP address.
- C. As R1 forwards the frame containing this packet, Sw-A will add 192.168.1.255 to its MAC table.
- D. R1 will encapsulate the packet in a frame with a destination MAC address of FF-FF-FF-FF-FFFF.
- E. As R1 forwards the frame containing this packet, Sw-A will forward it to the device assigned the IP address of 192.168.1.255.

2. Users on the 192.168.1.0/24 network must access files located on the Server 1.

What route could be configured on router R1 for file requests to reach the server?

- A. ip route 0.0.0.0 0.0.0.0 s0/0/0
- B. ip route 0.0.0.0 0.0.0.0 209.165.200.226
- C. ip route 209.165.200.0 255.255.255.0 192.168.1.250
- D. ip route 192.168.1.0 255.255.255.0 209.165.100.250

3. When a packet is sent from Host 1 to Server 1, in how many different frames will the packet be encapsulated as it is sent across the internetwork?

- A. 0
- B. 1
- C. 2
- D. 3
- E. 4

4. What must be configured on the network in order for users on the Internet to view web pages located on Web Server 2?

- A. On router R2, configure a default static route to the 192.168.1.0 network.
- B. On router R2, configure DNS to resolve the URL assigned to Web Server 2 to the 192.168.1.10 address.
- C. On router R1, configure NAT to translate an address on the 209.165.100.0/24 network to 192.168.1.10.
- D. On router R1, configure DHCP to assign a registered IP address on the 209.165.100.0/24 network to Web Server 2.

5. The router address 192.168.1.250 is the default gateway for both the Web Server 2 and Host 1. What is the correct subnet mask for this network?

- A. 255.255.255.0
C. 255.255.255.250
6. LAB:

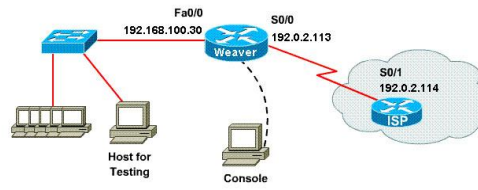
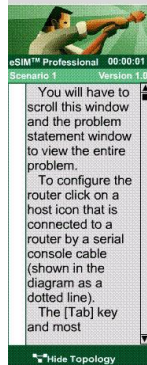
- B. 255.255.255.192
D. 255.255.255.252

The following have already been configured on the router:

- The basic router configuration
- The appropriate interfaces have been configured for NAT inside and NAT outside.
- The appropriate static routes have also been configured (since the company will be a stub network, no routing protocol will be required)
- All passwords have been temporarily set to "cisco".

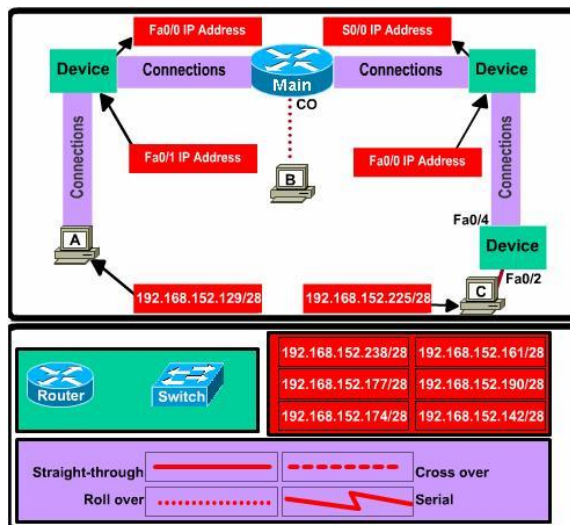
The task is to complete the NAT configuration using all IP addresses assigned by the ISP to provide Internet access for the hosts in the Weaver LAN. Functionality can be tested by clicking on the host provided for testing.

Configuration information
router name - Weaver
inside global addresses-198.184.105 198.184.110/29
inside local addresses - 192.168.100.17 - 192.168.100.30/28
number of inside hosts - 14



Please Input correct Answer here:

7. This topology contains 3 routers and 1 switch. Complete the topology.



Drag the appropriate device icons to the locations labeled Device.
Drag the appropriate connections to the locations labeled Connections.

Drag the appropriate IP addresses to the locations labeled IP address. (Hint : Use the given host addresses and the Main router information given)

To remove a device or connection , drag it away from the topology.

Use information gathered from the Main router to complete the configuration of any additional routers. No passwords are required to access the Main router. The config terminal command has been disabled for the HQ router. This router does not require configuration.

Drag and drop the network user application to the appropriate description of its primary use. (Not all options are used.)

e-mail	provides a way to look at and interact with information on the Internet
web browser	allows users to create and send text to other users in real time
instant message	allows users to send messages and files to users on or outside their network
IP telephony	allows users to store and retrieve information from a central location
collaboration	creates a space where users can interact on common projects
database	

Drag and drop question. Drag the items to the proper locations.



22.4 真题解答***

参照拓扑图，一个小的网络使用单一线路连接到 Internet，根据图中的信息，回答下面的问题。题 1~5 使用的是同一个拓扑图。

1. 解：B

题目问：如果路由器 R1 有一个包的目的地址是 192.168.1.255，哪一个描述了网络的操作？路由器 R1 有一个接口的 IP 地址是 192.168.1.250/24，该接口所在 IP 子网的广播地址是 192.168.1.255，在默认情况下，路由器丢弃所有去往广播地址的数据包，也称路由器有隔离广播作用。

2. 解：A

题目问：192.168.1.0/24 子网中的用户要访问 Server 1 上的文件，为了使文件请求能够到达服务器，R1 上需要配置什么路由？路由器 R1 是一个小网络的出口路由器，且只有单一线路连接到 Internet，为了使内部网络可以访问 Internet，需要在 R1 上配置一条默认路由。在串行线路上，静态路由和默认路由后可以跟下一跳路由器直连接口的 IP 地址，也可以跟本路由器的外出接口。

3. 解：D

题目问：当主机 1 发送一个包到 Server 1，这个包穿越互联网时，包需要被封装多少个不同的帧？主机 1 发出这个数据包前，需要先封装成帧。这个帧到达路由器 R1 以后，被解

封装，路由器 R1 查询路由表，再次把数据包封装，并发送给 R2。帧到达路由器 R2 以后，被解封装，路由器 R2 查询路由表，再次把数据包封装，并发送给 Server 1。在整个传输过程中，数据包被封装 3 次。

4. 解：C

为了使 Internet 上的用户能够访问 Web Server 2 上的网页，网络必须配置什么？注意到 Web Server 2 使用的是一个私有地址，让外界可以访问到这个私有地址上的网页，需要配置静态的 NAT，把私有地址转换成 209.165.100.0/24 子网中的一个合法地址；或者配置静态的 PAT，把一个合法地址的 80 端口静态映射到 192.168.1.10 的 80 端口。

5. 解：A

题目问：路由器接口的 IP 地址 192.168.1.250 是 Web Server 2 和主机 1 的默认网关，这个网络中的子网掩码是多少？这个题目出得不好，因为图中已经明确标出了“/24”，如果图中没有标出，读者也可以推导出来，因为 192.168.1.10、192.168.1.106、192.168.1.250 这三个 IP 地址处在同一个子网中，这个子网中的 IP 地址数量至少是 $250-10+1=249$ ，如果主机位的位数是 7 位，则只能容纳 126 台主机，不能满足要求；主机位的位数至少需要 8 位，网络则需要 24 位，对应的子网掩码是 255.255.255.0。

6. 解

本题是一个实验题，要求考生输入相应的命令。题目说，路由器上下列的信息已经被配置了：

- 路由器的基本配置；
- 适当的接口也被配置了 NAT outside 和 NAT inside；
- 适当的静态路由也被配置了（因为这个公司是一个存根网络，不需要配置动态路由协议）；
- 所有的密码都被临时设置成 cisco。

任务是完成 NAT 配置，使用 ISP 分配的所有 IP 地址提供 Weaver 局域网中的主机访问 Internet，可以在局域网的 Testing 主机上测试配置是否成功。

要配置的任务有：

- 路由器的名字是 Weaver；
- 内部全局地址是 198.18.184.105~198.18.184.110/29；
- 内部本地地址是 192.168.100.17~192.168.100.30/28；
- 内部有 14 台主机。

Console 主机使用配置线缆与 Weaver 路由器相连，单击 Console 主机而不是单击 Weaver 路由器，开始对路由器进行配置。如果想查看拓扑，只要关闭刚打开的配置窗口就可以了；如果想继续配置，只需单击 Console 主机即可。注意：如果路由器提示输入密码，密码是题目中给出的 cisco。配置如下：

```
Router>en
Router#config terminal
Router(config)#hostname Weaver
Router(config)#ip nat pool test 198.18.184.105 198.18.184.110 netmask 255.255.255.248
Router(config)#ip nat inside source list 1 pool test
Router(config)#access-list 1 permit 192.168.100.16 0.0.0.15
Router(config)#int s0/0
```

```
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config-if)#int fa0/0
Router(config-if)#ip nat inside
```

配置完成后, 在 Testing 主机上 ping ISP 的地址 192.0.2.114, 如果可以成功 ping 通, 表示配置成功。记得使用 “write” 或 “copy run start” 命令保存路由器的配置。

7. 解:

这是一个拖拉题。题目说, 拓扑中包含了 3 台路由器、1 台交换机, 要求完成拓扑:

- 把适当的设备 (也就是图中的路由器或交换机) 拖到有 Device 标签 (3 个设备) 的位置。
- 把适当的连接线 (也就是图中出现的 4 种线: 直通、交叉、全反和串行线) 拖到有 Connections 标签 (4 条线缆) 的位置。
- 把适当的 IP 地址 (也就是图中给出的 6 个 IP 地址) 拖到有 IP Address 标签 (4 个 IP 地址) 的位置。

提示: 可以使用图中给出的主机地址以及 Main 路由器的输出。

如果发现拖错了位置, 只要把设备、连线或 IP 地址拖出拓扑图即可。使用从 Main 路由器收集的信息完成配置。Main 路由器没有配置密码, 其他路由器不需要配置, 被禁用了终端。

解题思路如下:

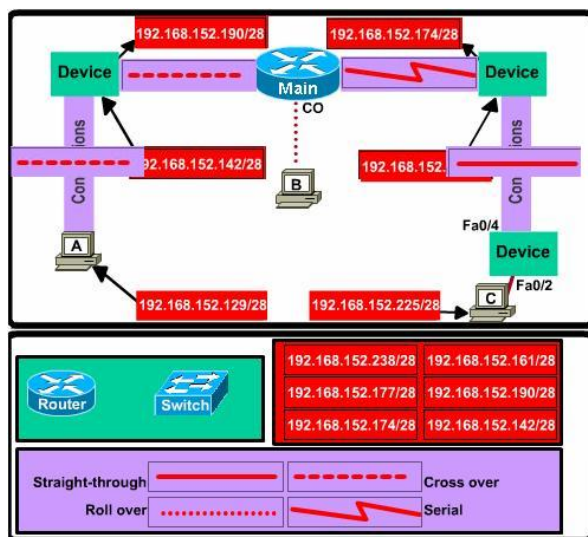
拖设备: 从图中可以看出, 有两台设备两个接口都需要配置 IP 地址, 知道 Main 路由器左右两台设备都是路由器, 因为交换机是二层的, 每个接口不能配置 IP 地址, 剩下的那台设备就是交换机了。满足 3 台路由器、1 台交换机。

拖连线: 计算机和路由器属于同种设备, 主机 A 上面的连线是交叉线。Main 与左边的路由器通过以太网接口相连, 使用的是交叉线。Main 路由器与右边的路由器通过串行口相连, 使用的是串行线。路由器和交换机之间的以太网连线使用直通线。计算机和交换机之间的以太网连线使用直通线。

拖 IP 地址标签: 与主机 A 相连的路由器接口的 IP 地址范围是 192.168.152.129~143/28, 192.168.152.142/28 满足要求。与主机 C 相连的路由器接口的 IP 地址范围是 192.168.152.225~239/28, 192.168.152.238/28 满足要求。接下来的两个 IP 地址可以根据 Main 路由器接口的 IP 地址来判断, 单击主机 B, 输入 “show running-config” 命令查看 Main 路由器的输出, 关键部分显示如下:

```
Main>enable
Main#show run
interface FastEthernet0/0
 ip address 192.168.152.177 255.255.255.240
!
interface Serial0/0
 ip address 192.168.152.161 255.255.255.240
 clockrate 64000
```

从上面的输出中可知, 与 Main 的 Fa0/0 接口相连接口的 IP 地址范围是 192.168.152.177~190/28, 192.168.152.190/28 满足要求。与 Main 的 S0/0 接口相连接口的 IP 地址范围是 192.168.152.161~174/28, 192.168.152.174/28 满足要求。



8. 解:

这是一个拖拉题，把左边选项拖到右边的描述中。正确答案如下图所示。

Drag and drop the network user application to the appropriate description of its primary use. (Not all options are used.)

e-mail	web browser
web browser	instant message
instant message	e-mail
IP telephony	database
collaboration	collaboration
database	



《CCNA 学习与实验指南》读者交流区

尊敬的读者：

感谢您选择我们出版的图书，您的支持与信任是我们持续上升的动力。为了使您能通过本书更透彻地了解相关领域，更深入的学习相关技术，我们将特别为您提供一系列后续的服务，包括：

1. 提供本书的修订和升级内容、相关配套资料；
2. 本书作者的见面会信息或网络视频的沟通活动；
3. 相关领域的培训优惠等。

请您抽出宝贵的时间将您的个人信息和需求反馈给我们，以便我们及时与您取得联系。

您可以任意选择以下三种方式与我们联系，我们都将记录和保存您的信息，并给您提供不定期的信息反馈。

1. 短信

您只需编写如下短信：B11572+您的需求+您的建议

发送到1066 6666 789（本服务免费，短信资费按照相应电信运营商正常标准收取，无其他信息收费）
为保证我们对您的服务质量，如果您在发送短信24小时后，尚未收到我们的回复信息，请直接拨打电话（010）88254369。

2. 电子邮件

您可以发邮件至jsj@phei.com.cn或editor@broadview.com.cn。

3. 信件

您可以写信至如下地址：北京万寿路173信箱博文视点，邮编：100036。

如果您选择第2种或第3种方式，您还可以告诉我们更多有关您个人的情况，及您对本书的意见、评论等，内容可以包括：

- （1）您的姓名、职业、您关注的领域、您的电话、E-mail地址或通信地址；
- （2）您了解新书信息的途径、影响您购买图书的因素；
- （3）您对本书的意见、您读过的同领域的图书、您还希望增加的图书、您希望参加的培训等。

如果您在后期想退出读者俱乐部，停止接收后续资讯，只需发送“B11572+退订”至10666666789即可，或者编写邮件“B11572+退订+手机号码+需退订的邮箱地址”发送至邮箱：market@broadview.com.cn 亦可取消该项服务。

同时，我们非常欢迎您为本书撰写书评，将您的切身感受变成文字与广大书友共享。我们将挑选特别优秀的作品转载在我们的网站（www.broadview.com.cn）上，或推荐至CSDN.NET等专业网站上发表，被发表的书评的作者将获得价值50元的博文视点图书奖励。

我们期待您的消息！

博文视点愿与所有爱书的人一起，共同学习，共同进步！

通信地址：北京万寿路 173 信箱 博文视点（100036） 电话：010-51260888

E-mail: jsj@phei.com.cn, editor@broadview.com.cn

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：(010) 88254396；(010) 88258888

传 真：(010) 88254397

E-mail: dbqq@phei.com.cn

通信地址：北京市万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036